The Ultimate Step By Step Field Guide For Proxmox In The Real World...!!!

Lee R. Surber

Virtualization Complete

Business Basic Edition

Proxmox-freeNAS-Zentyal-pfSense

- Complete Multi-Role Business Solution With PDC, BDC, NAS, & Managed Endpoint/Router!
- Step-By-Step Including ALL The Command Line Entries You'll EVER Need!
- System Diagrams: Featuring Innovative Router Migration Scheme!

The ONLY Collection Available To Offer Such A COMPLETE Working Business Solution!

Virtualization Complete

Business Basic Edition

Proxmox-freeNAS-Zentyal-pfSense

By Lee R. Surber

Book Description

The Ultimate Step By Step Field Guide For Proxmox In The Real World...!!!

Learn the secrets of building a ***bulletproof*** virtual IT infrastructure. This ***4-In-1 collection*** leverages the ***power*** and ***cost effectiveness*** of open source Linux, delivering a ***complete solution in easy step-by-step format***. All the software components of this system are ***time tested*** in ***production*** and were chosen because they are simply the **BEST** at what they do. This field guide is ***easy*** enough for ***Linux beginners*** yet ***advanced*** enough for ***IT professionals!*** Select your system model, then, deploy it quickly with ***full diagrams*** and **ALL** the necessary ***command line entries*** provided for you!

- Leverage the bare metal **Proxmox** hypervisor to deploy a completely modular high performance foundation!
- Replace costly Cisco components with easily moveable virtual **pfSense** managed endpoints.
- Learn how to install high performance, redundant, semi-virtual **freeNAS** fileservers running the self-healing ZFS file system.
- Replace Microsoft active directory with robust **Zentyal** primary and backup directory servers.
- Additional content covers directory based VPN authentication, IDS, Rsync, iSCSI, NFS, LVM, ZFS snapshot backups, hardware pass-through, 10 min. disaster recovery, best practices, and much more!
- Take complete control of your entire server rack through web-based management over secure VPN.

Virtualization Complete is the **ONLY** collection available to offer such a comprehensive working business solution!

Copyright

Linux Solutions(LRS-TEK)

Virtualization Complete

Business Basic Edition

Proxmox-freeNAS-Zentyal-pfSense

Copyright © 2016 By Lee R. Surber Linux Solutions(LRS-TEK)

All rights reserved. No part of this publication may be reproduced, distributed, or transmitted in any form or by any means, or stored in a database or retrieval system, without the prior written permission of the publisher.

Linux Solutions(LRS-TEK)
3000 CR 615
Alvarado, TX 76009
Email: lee.surber@linuxsolutions.us

Visit our website at www.linuxsolutions.us

eBook 1st Edition

TABLE OF CONTENTS

Book Description
Copyright
.1-Introduction
.2-Before You Begin
.3-Best Practices
- .3.1-Hybrid Servers
- .3.2-Disaster Recovery
- .3.3-KVM Preferred
- .3.4-Small Footprint Virtualization
- .3.5-Clustering
- .3.6-Maximize Performance
- .3.7-System Diagrams

Book 1: Proxmox VE
- 1.1-Introduction To Proxmox
- 1.2-Installing Proxmox
- 1.3-Initial Login
- 1.4-Network Adapters
- 1.5-Adding LVM Storage
- 1.6-Configure LVM Storage
- 1.7-Configure NFS Storage
- 1.8-Configure iSCSI Storage
- 1.9-Creating VM Configurations
- 1.10-VM Backup & Restore
- 1.11-VM Hardware
- 1.12-Adding Pass-Through Disks
- 1.13-Troubleshooting Proxmox
- 1.14-Upgrading Proxmox

Book 2: pfSense
- 2.1-Introduction To pfSense
- 2.2-Installing pfSense
- 2.3-Assigning Network Interfaces
- 2.3-Assigning IP Addresses

2.4-Reset Admin Password
2.5-Web Configuration Wizard
2.6-Changing Themes
2.7-Configure DHCP Server
2.7.1-WINS, DNS, Gateway, and Domain
2.7.2-DHCP Client Reservations
2.8-Firewall Settings
2.8.1-LAN Rules
2.8.2-WAN Rules
2.9-OpenVPN
2.9.1-OpenVPN Client Export Utility
2.9.2-OpenVPN Setup Wizard
2.9.3-OpenVPN Client Connectors
2.9.4-Authenticate Zentyal Domain Users
2.10-Snort IDS
2.10.1-Install Snort Package
2.10.2-Snort Global Settings
2.10.3-Snort Interfaces
2.10.4-Updating Threat Rules
2.10.5-Threat Rule Categories
2.10.6-Add Alerts To Suppression List
2.10.7-Block Offenders At Source
2.11-Configuration Backups
Book 3: freeNAS
3.1-Traditional Storage Fails
3.2-freeNAS & ZFS
3.3-Installing freeNAS
3.4-Add freeNAS Pass-Through Disks
3.5-Set Storage For No Backup
3.6-Start freeNAS Through The Console
3.7-Initial Login
3.8-freeNAS Navigation
3.9-Network Configuration
3.10-Users And Groups
3.10.1-Adding A New User

3.10.2-Adding A New Group
3.11-Add A ZFS Volume
3.12-Detach And Move Volumes
3.13-ZFS Datasets
3.14-ZFS Permissions
3.15-freeNAS Services
3.15.1-CIFS(Windows Sharing) Service
3.15.2-NFS(Linux Sharing) Service
3.15.3-iSCSI Target Service
3.15.4-Rsync(Backup) Service
3.15.5-SSH(Secure Shell) Service
3.16-Add Network Shares
3.16.1-NFS Shares
3.16.2-Windows Shares
3.16.3-iSCSI Target Shares
3.17-ZFS Snapshot Backups
3.18-Restore A Snapshot In Windows
3.19-Rsync Replication
3.19.1-Add The Rsync Push Task
3.19.2-Add The Rsync Module
3.19.3-Tips On Using Rsync
3.20-Domain Membership
3.20.1-Domain Permissions
3.21-Configuration Backups
Book 4: Zentyal Domain Controller
4.1-Introduction To Zentyal
4.2-Installing Zentyal
4.3-Initial Login
4.4-Initial Setup
4.5-Navigating Zentyal
4.6-Adding Users
4.7-Adding Groups
4.8-Additional Domain Controller
4.9-Shut Down & Reboot
4.10-Upgrading Zentyal

4.11-Joining Zentyal Domains
4.11.1-Workgroup Authentication
4.11.2-Join The Domain In Windows
4.12-Configuration Backups
.4-Final Thoughts And Thanks
.5-Additional Resources

.1-Introduction

After a decade of research and experimentation this book will reveal the secrets of building a ***bulletproof*** virtual IT infrastructure. It leverages the ***power*** and ***cost effectiveness*** of open source Linux, delivering a ***complete solution in easy step-by-step format***. Full ***system diagrams*** have also been included to help visualize your system! All the software components of this system are ***time tested*** in ***production*** and were chosen because they are simply the **BEST** at what they do. Ideally suited to the ***business environment***, this is the **ONLY** book available today that offers such a complete working solution!

.1.1-Who is this book designed for?

When writing this book I wanted to keep it ***simple*** enough for ***Linux beginners*** yet ***advanced*** enough conceptually that ***IT professionals*** would still find benefit. With ***all*** command line entries included and easy to read diagrams, **THIS IS** the field guide I had always hoped for when starting years ago in virtual infrastructure!

.1.2-What you will learn!

There are so many cookbook methods about virtualization today that you can quickly become overwhelmed. It's all too easy to end up with an overly complex system that ultimately performs poorly. The focus of this book is to keep installation and setup as simple as possible while still maintaining a very high level of performance and reliability. Upon completion you can be assured of the following:

- You will understand installation and setup of a multi-machine Linux powered ***virtual infrastructure***.
- You will learn how to install a virtual ***managed endpoint/router*** supporting 30 second migration between servers.
- You will learn how to configure world class ***intrusion detection*** that blocks offenders immediately. This also includes threats from smart phones and thumb drives!
- You will learn how to install virtual Linux based ***primary and backup domain controllers***. These controllers are fully compatible with Microsoft Active Directory.
- You will learn how to configure a ***VPN tunnel*** on your new virtual router.
- You will learn how to setup ***domain authentication*** for your virtual ***VPN*** server.
- You will learn how to install semi-virtualized ***hybrid fileservers*** using a simple ***hardware pass-through*** method.
- You will learn how to configure ***fileserver redundancy*** leveraging the power of Rsync.

- You will learn how to configure the ***self healing ZFS*** file system for ***sustained*** I/O rates between 30 and 60 **Megabytes/sec** using Gigabit adapters.
- You will learn how to leverage ***ZFS snapshot backups*** avoiding the need for expensive backup software.
- You will learn how ***EASY*** IT Administration really can be!

.1.3-Key features!

Most people do not want or welcome change unless the ***benefits*** are overwhelmingly ***positive***! You can be assured of the following:

- You will maintain ***full*** Microsoft ***compatibility***.
- You can use ***existing hardware*** in most cases.
- You will have even greater software compatibility.
- You will **NEVER** have to pay for licensing again.
- You can ***simplify*** management and ***reduce*** IT staff.
- You will have ***more security*** to protect against intrusion and attack.
- You will have ***mobile connectivity*** with your office.
- You will have complete ***web-based*** remote ***control*** of all your systems.
- You will have ***instant backups*** available.
- You will ***save 90%*** over traditional system costs.

.1.4-How easy is it to install?

Every component in my system is based off an ISO CD/DVD Distribution! Linux gurus may want to roll their own system but it really isn't needed. This approach ***simplifies system setup*** and ***reduces the knowledge required*** to get it all up and running!

.1.5-What Linux distributions are used in this system?

The following Linux distributions are what I have chosen after years of research and testing:

- **Proxmox VE** - for virtualization platform
- **pfSense** - for routing, firewalling, NAT, intrusion detection, and VPN
- **Zentyal Server** - for Samba based active directory
- **freeNAS** - for file storage using the robust ZFS file system

.1.6-I don't know Linux! It's too complicated!

Linux is complex! Even professionals need to reference documentation! For that reason I have ***included*** all the ***command line*** entries you will ever need. This truly is a step-by-step field guide! One of the key concepts here is to ***keep it simple***! Virtualized machines can be ***recovered in minutes*** if something goes wrong. There is no need for complex raid devices or network configurations! You can feel relaxed that you will have an extremely reliable high performance system when completed!

.2-Before You Begin

- You will need a copy of PuTTY installed on your workstation for some SSH session command line post-install changes. Putty can be downloaded here: PuTTY console
- You will need computers capable of running Proxmox. I recommend the best multi-core machines you can spare with at least 16-32Gb of Ram. The more cores and RAM the better. You will also want multiple gigabit network adapters and multiple hard drives for storage. 2 to 6 Terabytes of storage per Proxmox server would be nice.
- You will need one or more unmanaged Gigabit network switches for reliable high speed networking.
- Since you will be installing NAS storage on these machines make sure you have enough hard disks installed. Example: 1 x 500Gb disk for Proxmox, 1 x 500Gb disk for VM images, and 2 x 2Tb drives for NAS hardware pass-through.
- If you want to take advantage of VPN you will need an internet connection. Most residential providers use sticky IP connections, captive portal, and layer 2 hardware authorization. This essentially means you have a cheap static IP address and didn't even know it. If your IP changes....simply edit your DNS zone record to the new IP.

NOTE: I recommend detaching all hard disks and network adapters with the exception of the Proxmox OS drive and the primary network interface. You will re-enable these additional drives and network adapters after the install.

.3-Best Practices

While writing this book I had to make a decision where to put this section. I feel ***so strongly*** about my chosen methods that I decided to cover it right here in the beginning. No need to worry if you don't fully grasp some of these methods right now! As you progress they will be re-introduced and further explained, where they will make much more sense!

Over the years, as advancements came, I tested and deployed. I've tried HA, clustering, iSCSI backed storage, QCow vs Raw vs vmdk disk, OpenVz vs KVM, virtio drivers, and the list goes on! ***Along the way I learned some hard lessons!*** So, this section is dedicated to tips and tricks that will make your deployments super simple and maximize the use of your hardware. Here we go!

.3.1-Hybrid Servers

Take advantage of modern hardware by building hybrid platforms. Essentially, you create a virtualization host with a ***built in bare metal NAS server***. You install the NAS just like any other VM with its OS residing on a virtual disk. The actual storage drives will reside on a physical LVM array assigned through a technique known as **hardware pass-through**. This method provides very respectable data read/write performance! I have tested sustained throughput rates in the range of 30-60 **Megabytes/sec** using Gigabit adapters.

The biggest advantage is that your data is **NOT** stored in a virtual disk file! Even if you destroy the VM the ***data remains safe***! This approach maximizes the use of your hardware resource and makes management, maintenance, and disaster recovery **MUCH** easier!

For example: The following scenarios should help understand cost and benefit!

- **Scenario 1**: Let's assume you have 2 Proxmox servers, 2 brand(x) NAS/SANs, and 1 brand(x)Router. You have consumed 5 positions in your rack and you cannot use 3 of those positions for anything else. If a NAS or Router goes down due to hardware failure you **WILL** be down for **6-24hrs** at the minimum unless you have an exact duplicate laying around.
- **Scenario 2**: Let's assume you have 5 Proxmox servers un-clustered. You have consumed 5 positions in your rack and each position can host anything! Some or all of these could be hybridized using hardware pass-through for NAS drives and extra network adapters for routing. If any machine went down you simply transfer the hot-swap storage drives for the NAS to the next Proxmox server, map a couple network adapter Mac addresses for the Router, restore your virtual machine images, and ***you're back running in 15 minutes or less!*** It is also important to note that this method does NOT cripple Proxmox in any way with respect to other VM's you wish to install providing you have enough disk and network resources.

.3.2-Disaster Recovery

If any of your Proxmox servers go down the single most important item to recover will **ALWAYS** be your ***VM image backups***. Think of them as Master Recovery Images! Without these you are lost so it is important to have as many copies as possible! My preferred method is to select a NAS(virtualized or standalone) to use as my **primary *VM image backup* server**. This server will host the NFS image backup share to Proxmox. This share is manually replicated(only once during setup) to all other NAS servers in the system and synchronized on schedule using Rsync. If a machine goes down I can replace it, re-install Proxmox, re-install any NAS drives , re-map my NFS backups, and restore the VM images. Once again, ***you're back running in 15 minutes or less!*** This method has served me very well and is rock solid time tested!

KEEP A COPY ON THUMB-DRIVE: Another highly recommended tip is to copy your VM image backups to a thumb-drive or DVD then store them in a fireproof safe. You can easily map a read-only samba share of your VM image backups to be accessible from any windows machine or android phone. Using the small footprint method described below ensures your entire VM image backup archive will easily fit on a modern 64-128GB USB thumb-drive.

.3.3-KVM Preferred

Proxmox allows for 2 types of virtualization, KVM and OpenVZ. The key difference between the two, is that KVM is fully virtualized, where OpenVZ is partially virtualized. While OpenVZ does yield performance benefits over KVM, it loses in every other way. **My choice is to only use KVM**! I will always choose compatibility and easy disaster recovery over performance! If you require more performance get better hardware! You can easily build a water-cooled over-clocked rocket with 8 or more cpu cores and 32Gb or more RAM on the cheap today!

.3.4-Small Footprint Virtualization

My preferred approach is what I term ***small footprint virtualization***. Let's assume you have a 2008 Windows Server with a need for 500GB capacity. There are 2 installation approaches that will work!

- **Scenario 1**: You could create a VM with virtual disks totaling 500GB. With this method you're looking at large image backups that take a long time to complete! Should you need to move or recover using a backup image it will also take a long time to restore!
- **Scenario 2**: With ***small footprint virtualization*** you create a VM with as small a virtual disk as allowable, then use a network backed resource such as ***iSCSI from within the guest*** to map the additional capacity requirement. This method allows for super fast backup and restore at the expense of some performance.

In production environments the flexibility of ***small footprint virtualization*** exceeds any minor performance hits. It allows you to backup and restore a VM with large capacity mappings to another physical machine quickly. This comes in very handy if you need to pull a machine down for maintenance.

.3.5-Clustering

In this book I do not cover clustering because it does **NOT** fit the simplicity model. Clustering is great for managing a large number of servers from a single interface but does add complexity to the system! It also relies heavily on network backed storage which reduces overall VM performance levels compared to dedicated hardware installs. When a cluster breaks you may want to plan on an all-nighter! Keeping your Proxmox servers un-clustered still allows for most recoveries and moves within minutes!

.3.6-Maximize Performance

Another preferred approach I will share based on experience should be a no-brainer. Any VM will perform better if it has ***dedicated*** disk and network ***hardware***. If you can spare the extra disks and network adapters it is highly recommended!

I think a good general rule is to allow no more than 2 VM guests per physical device. One being a low throughput guest while the other can be high throughput. For example: a domain controller only handling authentication can easily share a disk and network adapter with a multi-domain email server. A multi-domain web server may not share resources well under load with a file server.

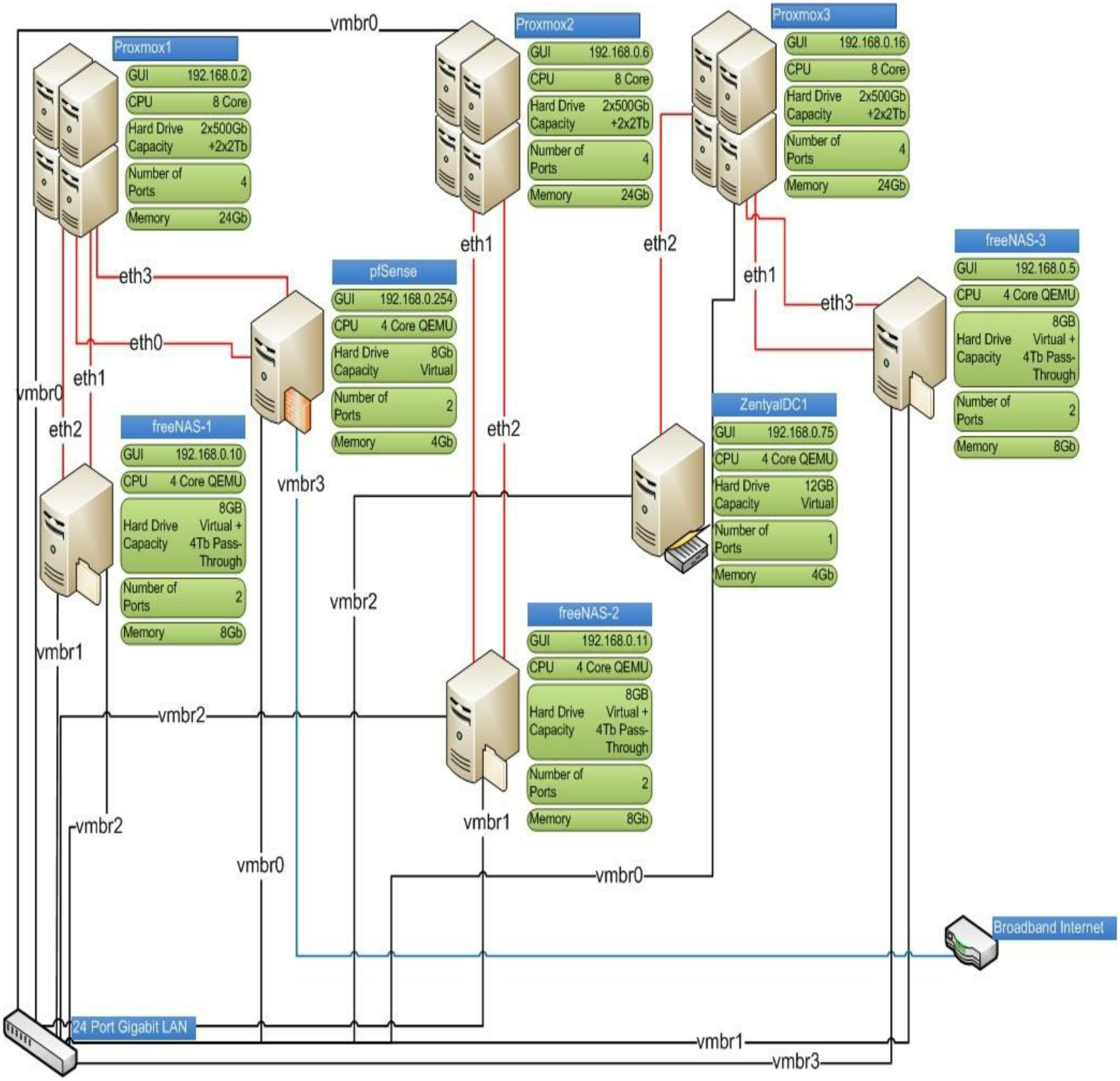
SSD DRIVES: I have had very good luck running up to 6 ***small footprint*** VM installs on just one SSD drive. Each one of these had dedicated network adapters!

AVOID NETWORK BACKED STORAGE IN PRODUCTION: This storage type is typically used by large enterprise with hundreds of servers where internet speed is the limiting factor and intermittent performance dynamics are expected. It relies on various protocols such as GlusterFS, RBD, iSCSI, and NFS. The **iSCSI** protocol is by far the most common and versatile of these for small to medium sized deployments. While **iSCSI** does work and is useful for testing environments, the performance is **NOT** on par with installs to ***local dedicated hardware***. Over a 10 year period I tried **EVERY** conceivable configuration in an environment with **VERY** respectable resources! My conclusion: If you **MUST** install a network backed VM it's because you failed to build your system with enough storage or you don't have enough Proxmox servers available! If you're going to map iSCSI targets do it ***from within a guest VM*** running on dedicated hardware! You will have respectable performance and you will **GAIN** hugely in backup and recovery management.

.3.7-System Diagrams

(Option-1) Optimal Hardware Benefit

The drawing below shows a system with 3 hybrid Proxmox servers. It is designed to maximize resources by making use of **ALL** available physical machines! **EVERY** virtual machine is installed on ***dedicated*** disk and network hardware for best production performance. VM installation to network backed storage(iSCSI and NFS) can still be used for temporary lower performance requirements.



freeNAS-1 Role In (Option-1) System

In this system **freeNAS-1** is setup as the primary NAS fileserver. It will host traditional Windows(CIFS), Linux(NFS), media, and ftp to your network clients. It will also host data related(NO BACKUP DRIVES) iSCSI targets to be ***mapped from within guest operating systems***. All shares are manually replicated during setup to **freeNAS-2** and **freeNAS-3** where they are automatically synchronized once per hour using Rsync.

freeNAS-3 Role In (Option-1) System

In this system **freeNAS-3** is setup to serve special Proxmox NFS shares for Templates, Containers, ISO, and VM Image Backups. It will provide ***load balancing*** by hosting shares for network client

backups. This also includes backup related(NO DATA DRIVES) iSCSI targets to be ***mapped from within guest operating systems***. **freeNAS-3** can host iSCSI and NFS targets for Proxmox VM images but should be avoided due to weaker performance. All shares are manually replicated during setup to **freeNAS-1** and **freeNAS-2** where they are automatically synchronized once per hour using Rsync. **freeNAS-3** is ***only available*** to network clients for backup purposes.

IMPORTANT: There is a ***caveat!*** Since **freeNAS-3** is virtualized it will not be able to backup its own VM image! You MUST backup this VM image to a different NFS share hosted by freeNAS1(nfs.netbackups2) then use Rsync once again to automatically synchronize the dataset to all other nodes. NOTE: nfs.netbackups2 will ONLY be used for freeNAS-3 VM Image Backups while ALL other VM Image Backups will be sent to the nfs.netbackups share.

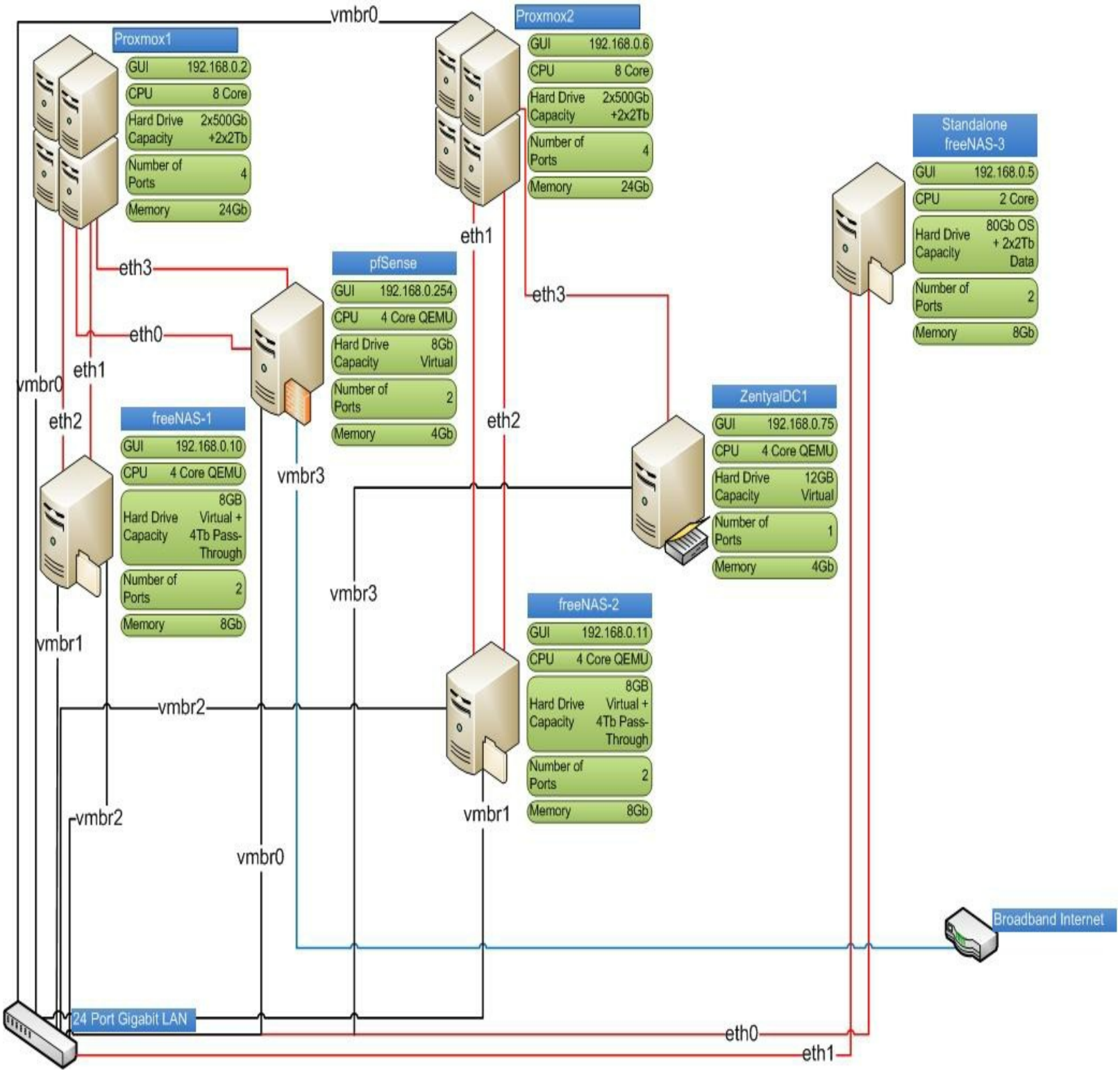
freeNAS-2 Role In (Option-1) System

freeNAS-2 does not host anything and is ***not available*** to network clients. It receives Rsync backups on schedule from **freeNAS-1** and **freeNAS-3** for disaster recovery usage. It could also be used to load balance by serving ***read only*** shares for files that don't change much.

With a little **Rsync** ***magic,*** all NAS servers end up containing the same datasets. The end result is a fully virtualized web administered business solution with 3 mirrored NAS servers, active directory, domain control, DHCP, DNS, firewall, intrusion detection, and VPN capability!

(Option-2) Optimized For Network Backed Storage

The drawing below shows a system with 2 hybrid Proxmox servers and 1 standalone NAS. It is designed to maximize network backed storage performance by making use of a ***standalone*** freeNAS server. Network backed storage is commonly used in larger clustered systems. It makes use of the iSCSI and NFS protocols enabling Proxmox to leverage remote storage. **EVERY** virtual machine should still be installed on ***dedicated*** disk and network hardware for best production performance. This system offers very acceptable performance when installing VM's on iSCSI or NFS targets. It also provides excellent image backup performance at the expense of using an entire slot in your server rack. There is once again a ***caveat*** here! ***If the standalone freeNAS-3 goes down do to hardware failure you may be down for 6hrs or more*** unless you have identical hardware to replace it with.



freeNAS-1 Role In (Option-2) System

In this system **freeNAS-1** is still setup as the primary NAS fileserver. It will host traditional Windows(CIFS), Linux(NFS), media, and ftp to your network clients. It will also host data related(NO BACKUP DRIVES) iSCSI targets to be ***mapped from within guest operating systems***. These shares are manually replicated during setup to **freeNAS-2** and **freeNAS-3** where they are synchronized once per hour using Rsync.

freeNAS-3 Role In (Option-2) System

In this system **freeNAS-3** is setup to serve special Proxmox NFS shares for Templates, Containers, ISO, and VM Image Backups. It will provide ***load balancing*** by hosting shares for network client

backups. This also includes backup related(NO DATA DRIVES) iSCSI targets to be ***mapped from within guest operating systems***. All shares are manually replicated during setup to **freeNAS-1** and **freeNAS-2** where they are automatically synchronized once per hour using Rsync. **freeNAS-3** is ***only available*** to network clients for backup purposes.

Main Difference: With ***bare-metal performance*** it can now be used to host iSCSI targets for Proxmox VM images. Using iSCSI multipath drivers with high quality network hardware yields very acceptable performance in critical testing environments.

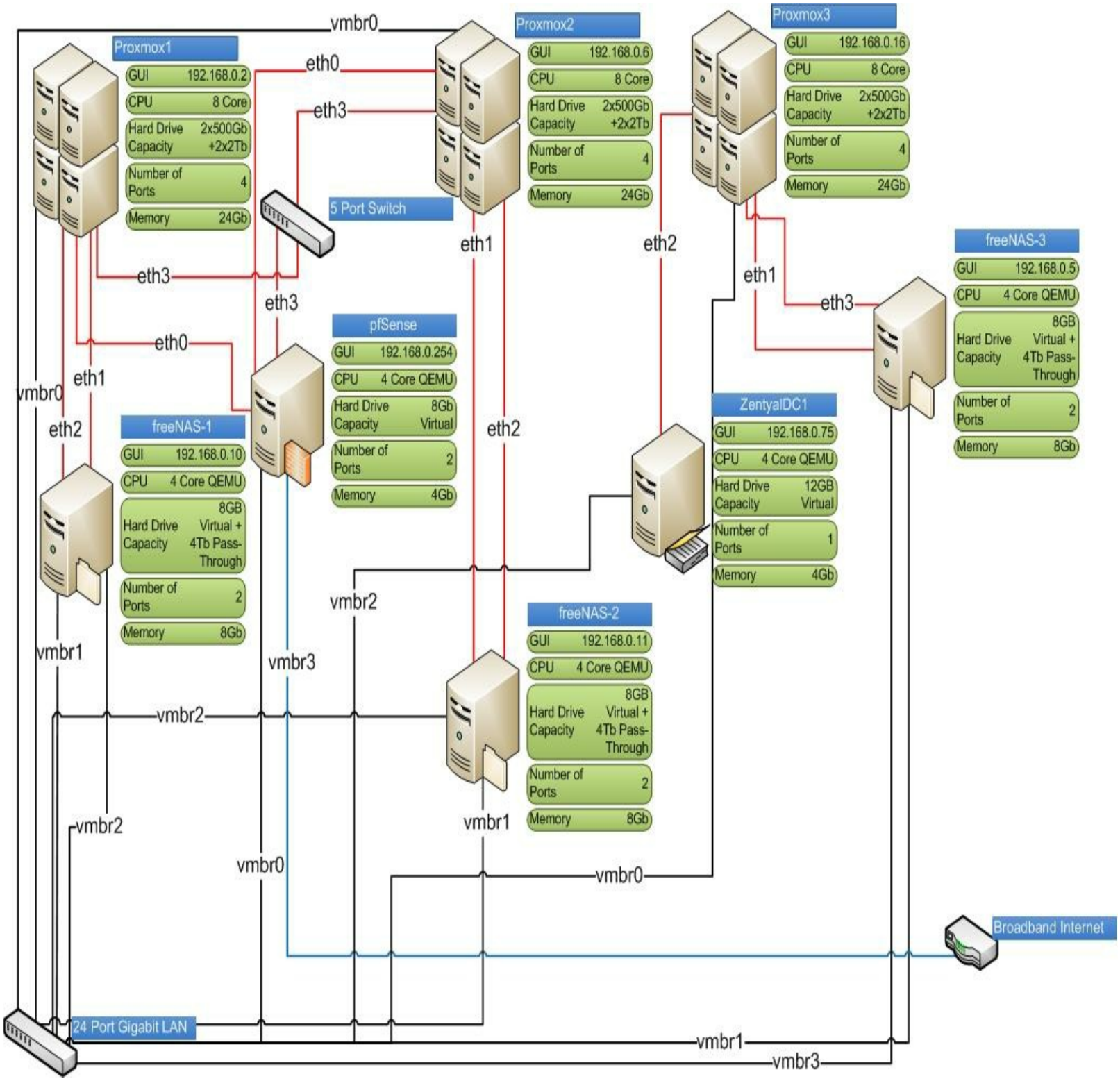
freeNAS-2 Role In (Option-2) System

In this system **freeNAS-2** does not host anything and is ***not available*** to network clients. It receives Rsync backups on schedule from **freeNAS-1** and **freeNAS-3** for disaster recovery usage. It could also be used to load balance by serving ***read only*** shares for files that don't change much.

With a little **Rsync *magic,*** all NAS servers end up containing the same datasets. The end result is a semi virtualized web administered business solution with 3 mirrored NAS servers, active directory, domain control, DHCP, DNS, firewall, intrusion detection, and VPN capability!

(Option-3) Easy Offline Router Migration

The drawing below shows a system with 3 hybrid Proxmox servers. With the addition of a simple 5 port switch and some well thought planning it is possible to move the pfSense router between Proxmox1 and Proxmox2. The system is designed to maximize resources by making use of **ALL** available physical machines! **EVERY** virtual machine is installed on ***dedicated*** disk and network hardware for best production performance. VM installation to network backed storage(iSCSI and NFS) can still be used for temporary lower performance requirements.



freeNAS-1 Role In (Option-3) System

In this system **freeNAS-1** is setup as the primary NAS fileserver. It will host traditional Windows(CIFS), Linux(NFS), media, and ftp to your network clients. It will also host data related(NO BACKUP DRIVES) iSCSI targets to be ***mapped from within guest operating systems***. All shares are manually replicated during setup to **freeNAS-2** and **freeNAS-3** where they are automatically synchronized once per hour using Rsync.

freeNAS-3 Role In (Option-3) System

In this system **freeNAS-3** is setup to serve special Proxmox NFS shares for Templates, Containers, ISO, and VM Image Backups. It will provide ***load balancing*** by hosting shares for network client

backups. This also includes backup related(NO DATA DRIVES) iSCSI targets to be ***mapped from within guest operating systems***. **freeNAS-3** can host iSCSI and NFS targets for Proxmox VM images but should be avoided due to weaker performance. All shares are manually replicated during setup to **freeNAS-1** and **freeNAS-2** where they are automatically synchronized once per hour using Rsync. **freeNAS-3** is ***only available*** to network clients for backup purposes.

IMPORTANT: There is a ***caveat!*** Since **freeNAS-3** is virtualized it will not be able to backup its own VM image! You MUST backup this VM image to a different NFS share hosted by freeNAS-1(nfs.netbackups2) then use Rsync once again to automatically synchronize the dataset to all other nodes. NOTE: nfs.netbackups2 will ONLY be used for freeNAS-3 VM Image Backups while ALL other VM Image Backups will be sent to the nfs.netbackups share.

freeNAS-2 Role In (Option-3) System

freeNAS-2 does not host anything and is ***not available*** to network clients. It receives Rsync backups on schedule from **freeNAS-1** and **freeNAS-3** for disaster recovery usage. It could also be used to load balance by serving ***read only*** shares for files that don't change much.

With a little **Rsync** ***magic,*** all NAS servers end up containing the same datasets. The end result is a fully virtualized web administered business solution with 3 mirrored NAS servers, active directory, domain control, DHCP, DNS, firewall, intrusion detection, and VPN capability!

Book 1: Proxmox VE

1.1-Introduction To Proxmox

With an active community and rock solid distribution Proxmox shines! You can download it in CD/DVD ISO format from the Proxmox website here: Proxmox VE For the purpose of this book I have used Proxmox VE 3.4. Once you have it downloaded , burn it to disk, insert it, and follow the simple installation routine. For those who aren't familiar Proxmox is a complete open source virtualization management platform. It offers enterprise class features such as HA, clustering, live migration, web management, and hardware pass-through capability. It also is capable of running on the newest ZFS file system and allows both KVM and Open VZ container virtualization types.

With advancements in modern hardware there is really no reason NOT to virtualize. It makes management and maintenance simple while affording greater compatibility lending to longer software/hardware life cycles.

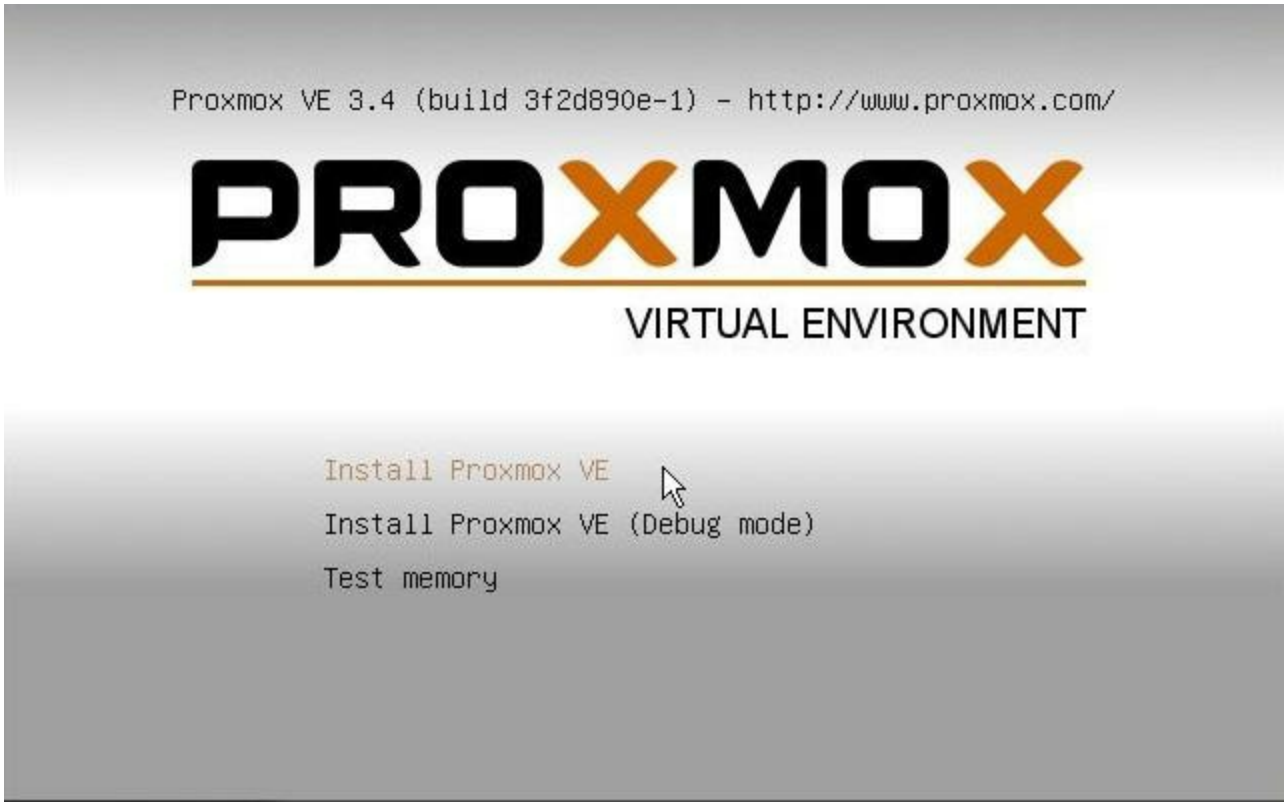
If you rely on Windows XP 32 bit for some over-priced software package you're no longer going to have to upgrade do to hardware failure on the physical machine. Simply virtualize that machine from backup!

NOTE: Proxmox is a powerful platform and it's feature-set cannot be completely covered in this book. This guide was designed as a step-by-step to get you up and running quickly. I highly recommend tapping the wealth of online resources available for a more thorough understanding.

1.2-Installing Proxmox

Insert the Proxmox disk and boot the machine. You will be greeted by the following window.

To continue: Press **Enter**



EULA

The next screen (shown below) contains the END USER LICENSE AGREEMENT (EULA). I know you will carefully read this from beginning to end! When finished reading:

To continue: Click **I Agree**

PROXMOX
INSTALLER

License

END USER LICENSE AGREEMENT (EULA)

END USER LICENSE AGREEMENT (EULA) FOR PROXMOX VIRTUAL ENVIRONMENT (PROXMOX VE)

By using Proxmox VE software you agree that you accept this EULA, and that you have read and understand the terms and conditions. This also applies for individuals acting on behalf of entities. This EULA does not provide any rights to Support Subscriptions Services as software maintance, updates and support. Please review the Support Subscriptions Agreements for these terms and conditions. The EULA applies to any version of Proxmox VE and any related update, source code and structure (the Programs), regardless of the the delivery mechanism.

1. License. Proxmox Server Solutions GmbH (Proxmox) grants to you a perpetual, worldwide license to the Programs pursuant to the GNU Affero General Public License V3. The license agreement for each component is located in the software component's source code and permits you to run, copy, modify, and redistribute the software component (certain obligations in some cases), both in source code and binary code forms, with the exception of certain binary only firmware components and the Proxmox images (e.g. Proxmox logo). The license rights for the binary only firmware components are located within the components. This EULA pertains solely to the Programs and does not limit your rights under, or grant you rights that supersede, the license terms of any particular component.

2. Limited Warranty. The Programs and the components are provided and licensed "as is" without warranty of any kind, expressed or implied, including the implied warranties of merchantability, non-infringement or fitness for a particular purpose. Neither Proxmox nor its affiliates warrants that the functions contained in the Programs will meet your requirements or that the operation of the Programs will be entirely error free, appear or perform precisely as described in the accompanying documentation, or comply with regulatory requirements.

3. Limitation of Liability. To the maximum extent permitted under applicable law, under no circumstances will Proxmox, its affiliates, any Proxmox authorized distributor, or the licensor of any component provided to you under this EULA be liable to you for any incidental or consequential damages, including lost profits or lost savings arising out of the use or inability to use the Programs or any component, even if Proxmox, its affiliates, an authorized distributor and/or licensor has been advised of the possibility of such damages. In no event shall Proxmox's or its affiliates' liability, an authorized distributor's liability or the liability of the licensor of a component provided to you under this EULA exceed the amount that you paid to

Abort

I agree

Configuring The Hard Disk

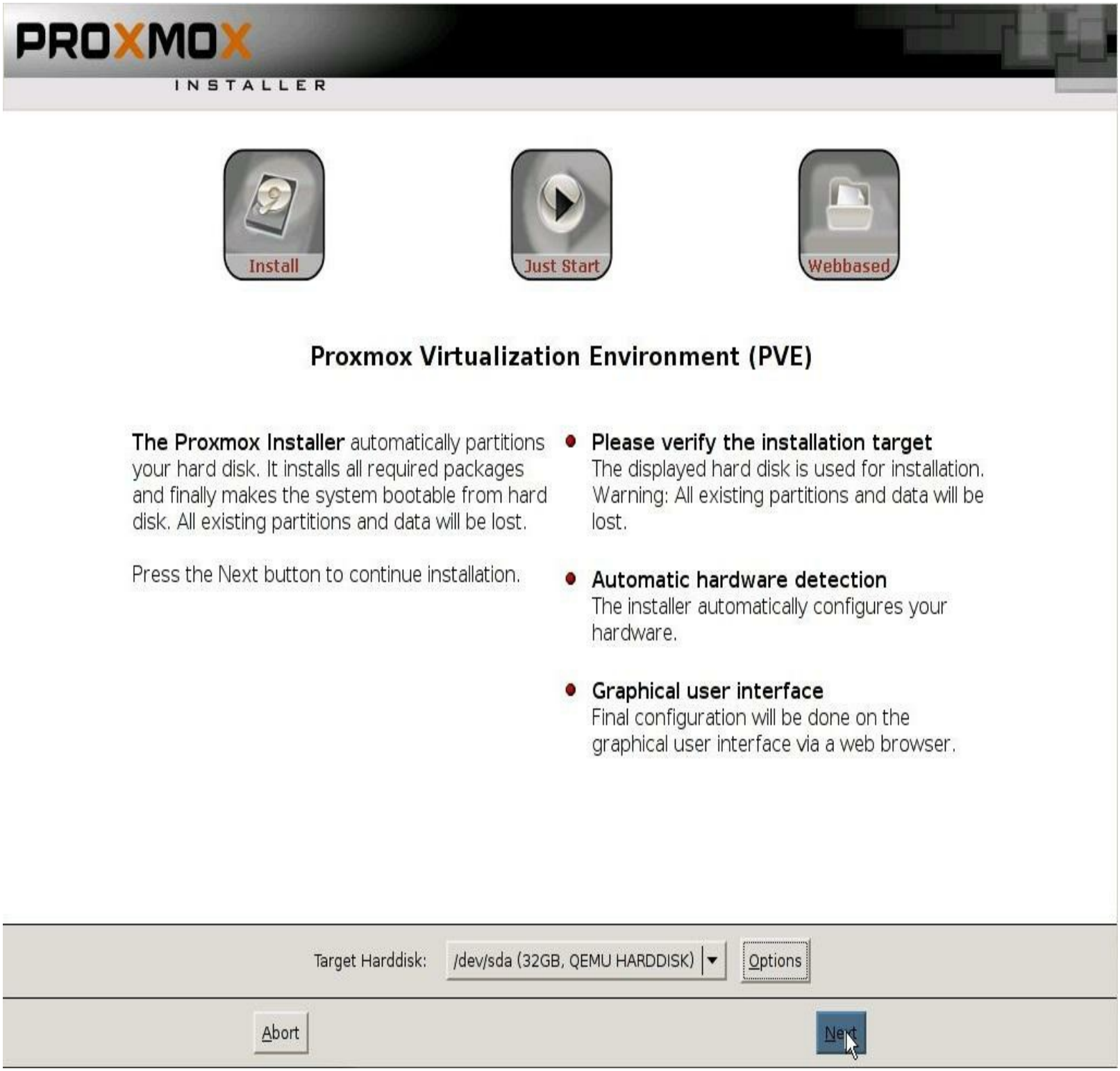
This step assumes a simple install with one drive and no raid. My personal preference here is to only have one disk attached to the motherboard for a fresh install. Just detach all disks with exception of the one used for the OS. This avoids any possible MBR issues if you ever need to remove disks due to failure. It's easy to get confused if you have multiple hard disks installed in any machine. For this reason I like to include a hard disk ID map. This can be as simple as a sticky note or magic marker ID's on each disk.

NOTE: It has been long advised by the Proxmox developers to only install to a single disk partitioned and managed by LVM. Raid has not been supported until recently. My personal opinion

is that raid really doesn't matter. A properly maintained system will always be pulled from service before a catastrophic disk failure happens. There are **ALWAYS** warning signs! From an engineering perspective a parity array such as **RAID(1, 5, 6, or 10)** introduces extended duty cycles and heat buildup thus shortening motor life. A striping array such as **RAID-0** reduces duty cycles and heat buildup thus increasing motor life. It also provides increased throughput as a bonus! It is the only RAID I use for these stated reasons!

Back to the install! By clicking the options button below you will notice that Proxmox now allows for ZFS raid configuration. As mentioned above I do not use this but it is an option if you desire. If you are following my instructions, which you should be, we will be performing a default installation to the primary target disk (/dev/sda) so close the options dialog if you opened it.

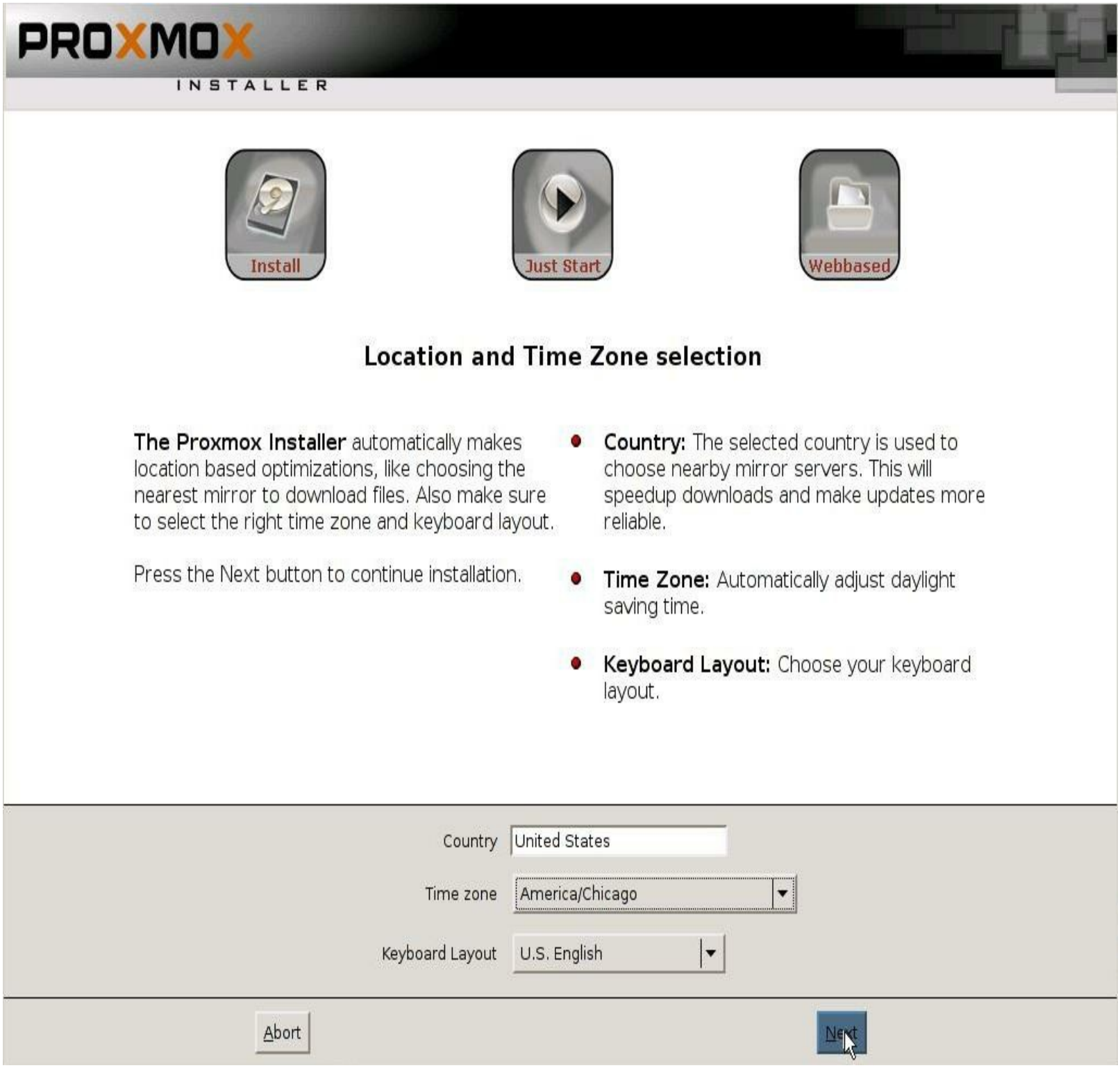
To continue: Click **Next**



Choose Your Location And Time

Next you will setup your default location and time zone.

To continue: Click **Next**



Root Password And Email Address

Now you will set your root password and email address. Make sure to use a strong root password!

To continue: Click **Next**

PROXMOX INSTALLER

Install | Just Start | Webbased

Administration Password and E-Mail Address

Proxmox Virtual Environment is a full featured GNU/Linux system based on Debian. Therefore you should use a strong password with at least 5 characters.

All administrative emails are sent to the specified address.

Press the Next button to continue installation.

- **Password:** Please use strong passwords. Your password should be 8 or more characters in length. Also combine letters, numbers, and symbols.
- **E-Mail:** Administrator email address.

Password ●●●●●●●

Confirm ●●●●●●●

E-Mail yourname@yourwebs.com

Abort | Next

Network Configuration

Next you will setup your network. Your settings should look something like this(where x can be substituted for any number between 0 and 255):

FQDN: proxmox1.yourdomain.com

IP Address: 192.168.x.2

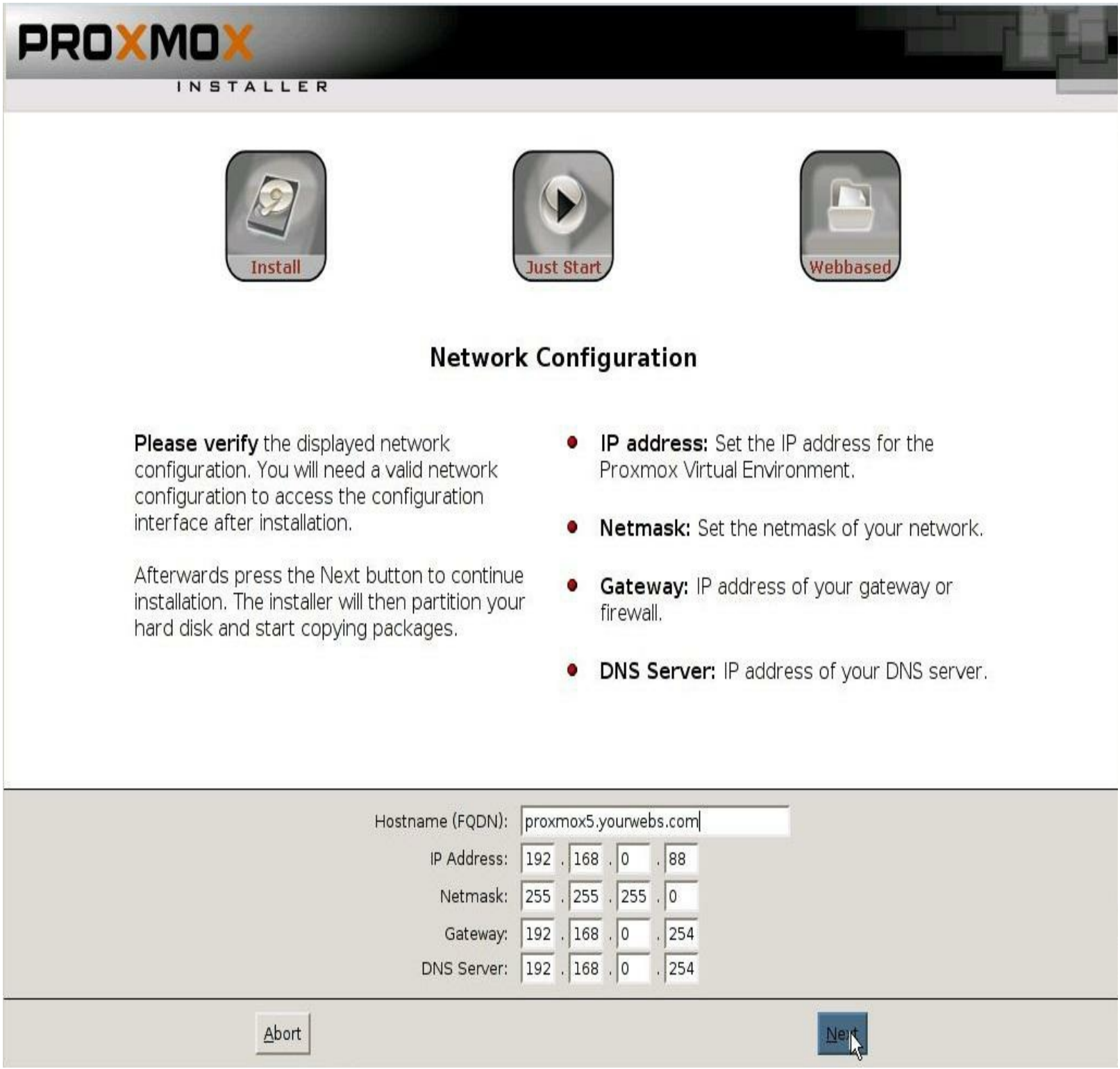
Netmask: 255.255.255.0

Gateway: 192.168.x.254

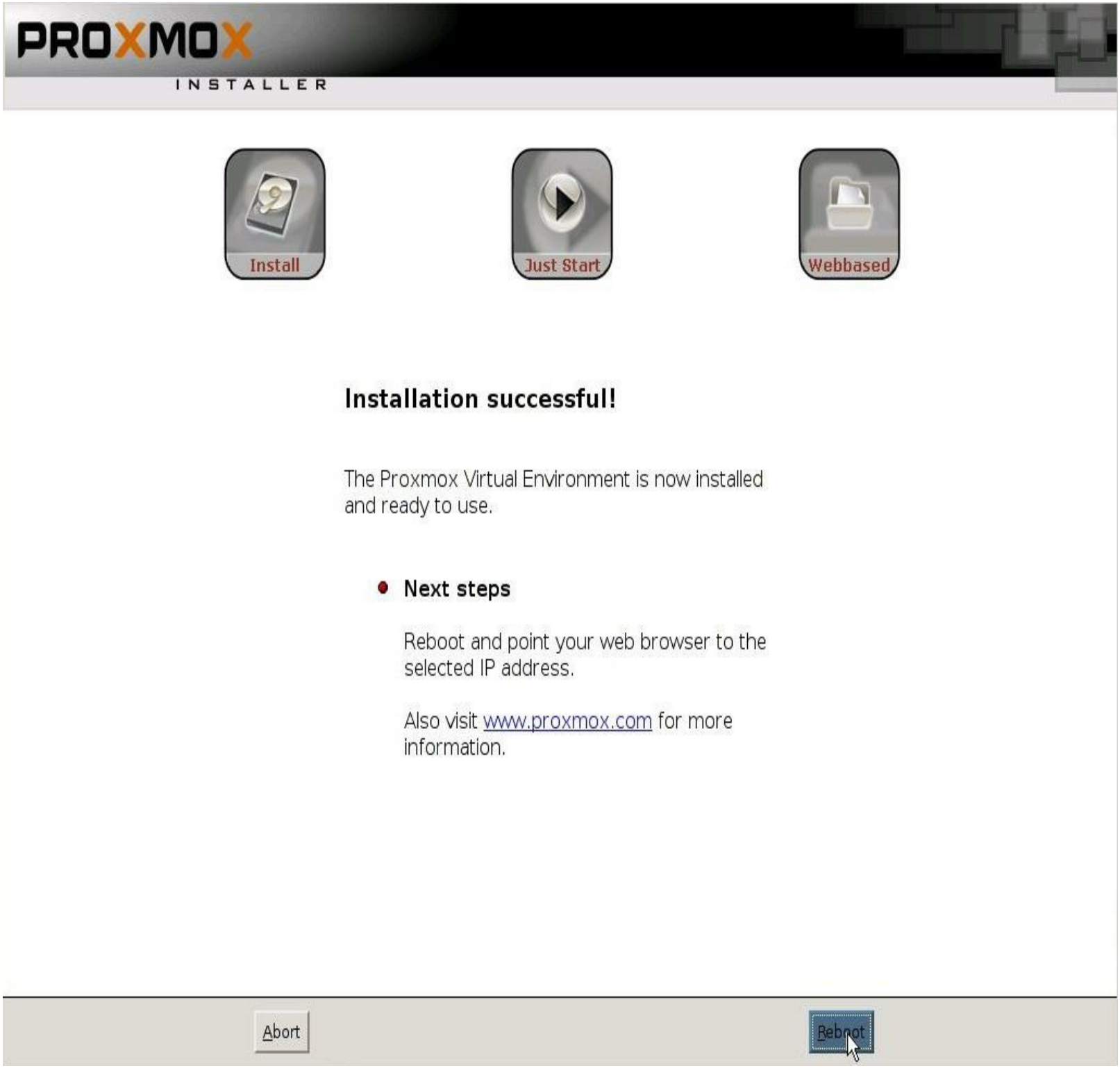
DNS: 192.168.x.254

NOTE: We choose 192.168.x.254 for both gateway and DNS because it lies outside the DHCP address range defaults(192.168.x.100-192.168.x.200) on most routers. For specific rules on private IP addressing do an internet search for RFC 1918 guidelines. I highly recommend using pfSense for a managed endpoint/routing platform! I have used it for 7 years virtualized without incident! It will handle all DHCP, DNS, NAT, VPN, and Intrusion Detection. You can download it here: [pfSense router]

To continue: Click **Next**



To continue: Click **Reboot**



PLEASE NOTE: When Proxmox reboots take note of the address for logging in to the web interface. It should match the address set in the previous network configuration screen.

Example: https://192.168.10.2:8006

At this point you need to login as ***root*** using the ***password*** you provided during installation and issue a shutdown. The command is shown below. Only type the word poweroff followed by the **Enter** key.

poweroff

HIGHLY RECOMMENDED: Once the machine powers down you will install any additional network adapters and hard disks. I recommend labeling the network adapters used in the system with MAC/Hardware address. If you are not familiar with MAC/hardware addresses they usually look something like this 92:26:b9:c2:42:15 and should be clearly identified on your device. You need the ability to identify each network port externally using its MAC. I personally write the last 4 digits of the MAC on each adapter bracket with magic marker for easy identification.

I have found that some USB network adapters do work well and will be pre-labeled with ID and serial. I use these for low bandwidth connections such as the pfSense router.

When finished start the machine for the next step in the setup.

1.3-Initial Login

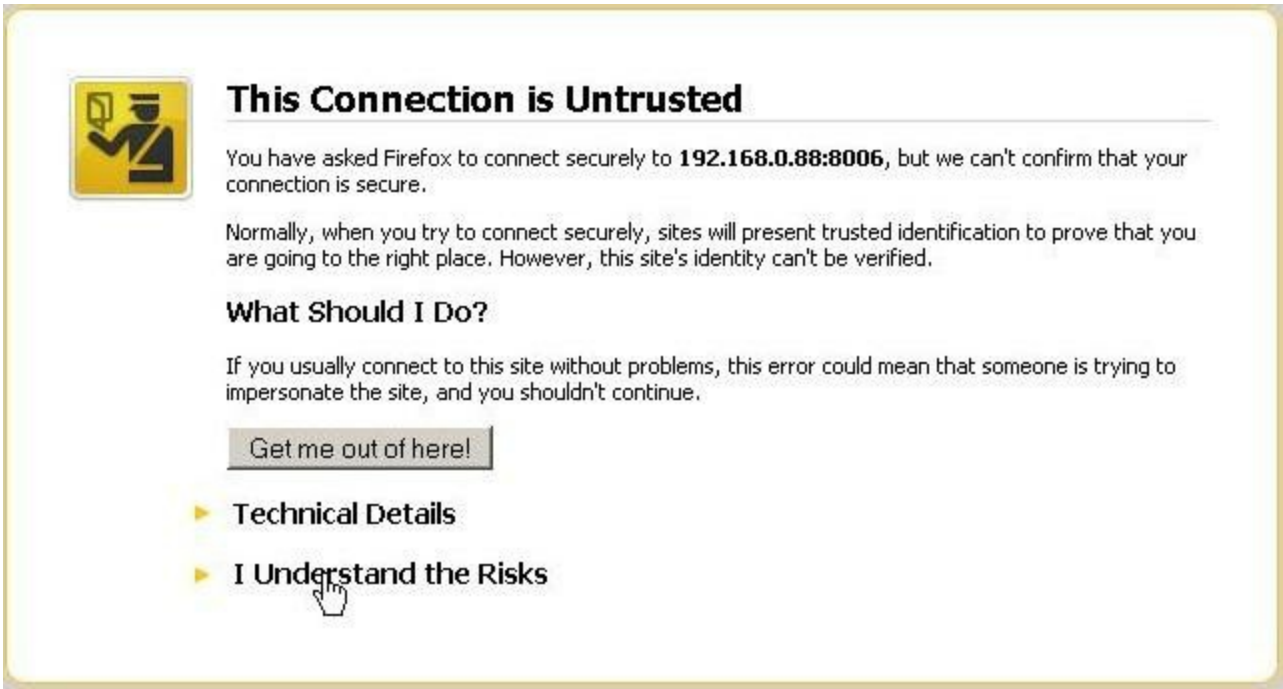
Now the you have completed the install it is time to login. Open your favorite web browser (I use Mozilla Firefox) then enter the ip address you chose during installation.

Please Note: Proxmox uses secure port 8006 by default

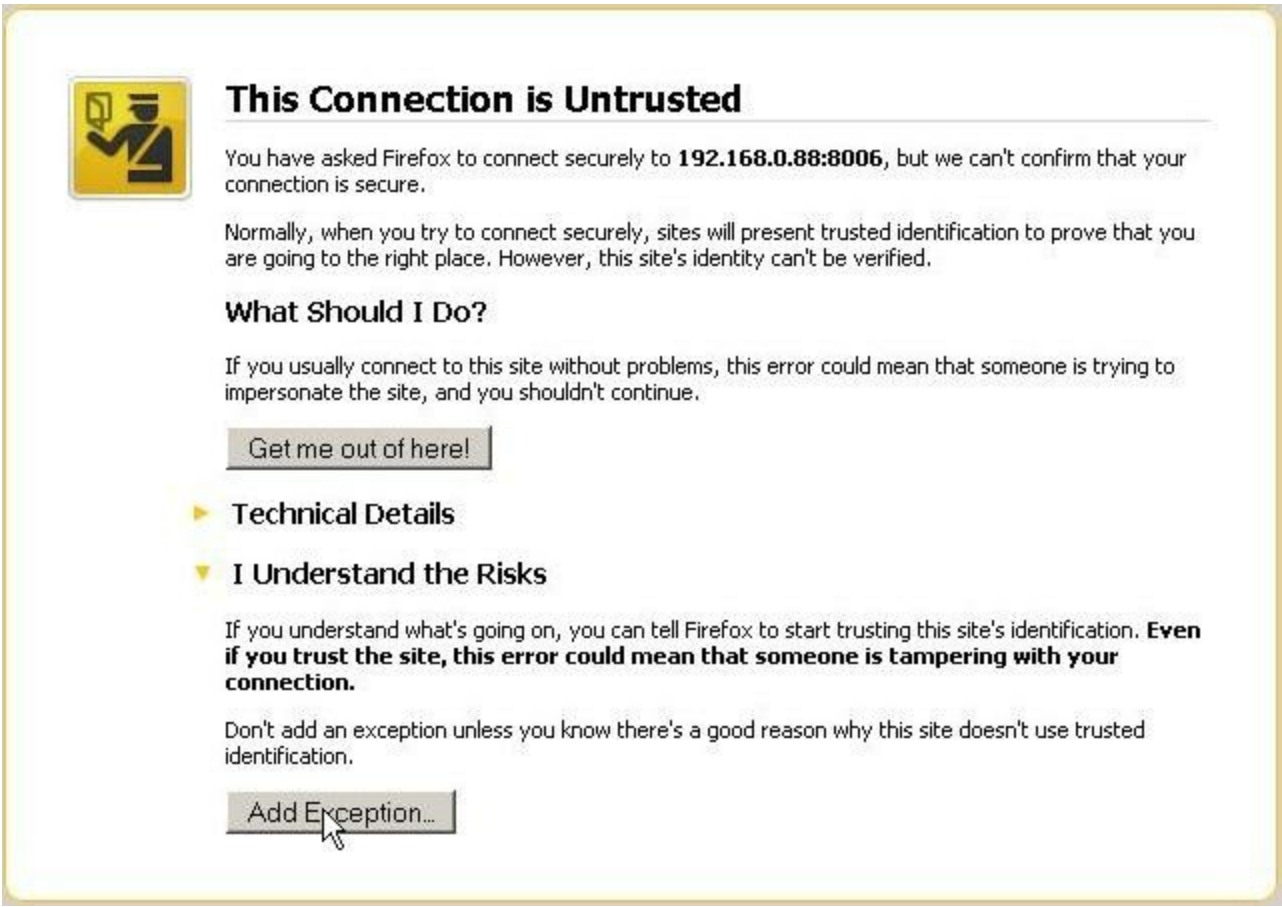
Your entry should look something like this:

https://192.168.10.2:8006

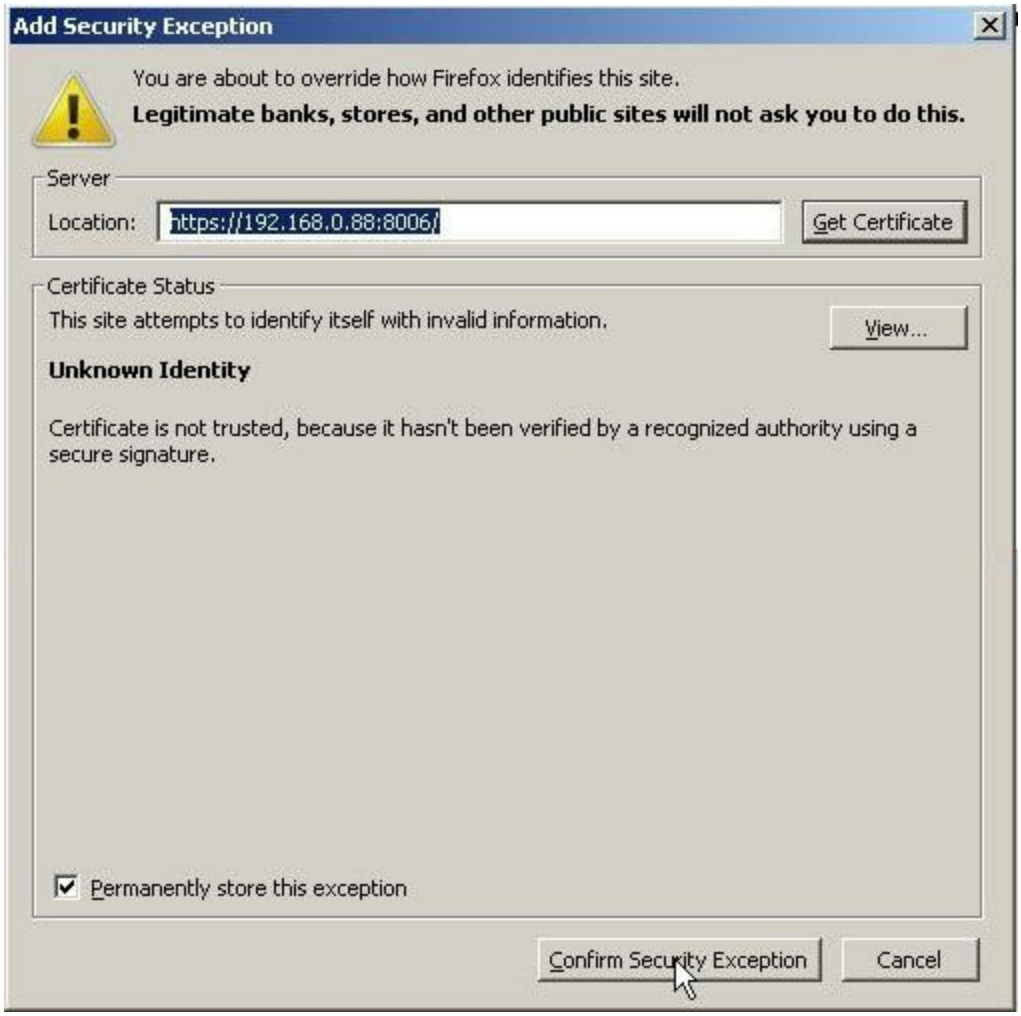
You will then see a secure connection warning as pictured below. Click ***I Understand the Risks***



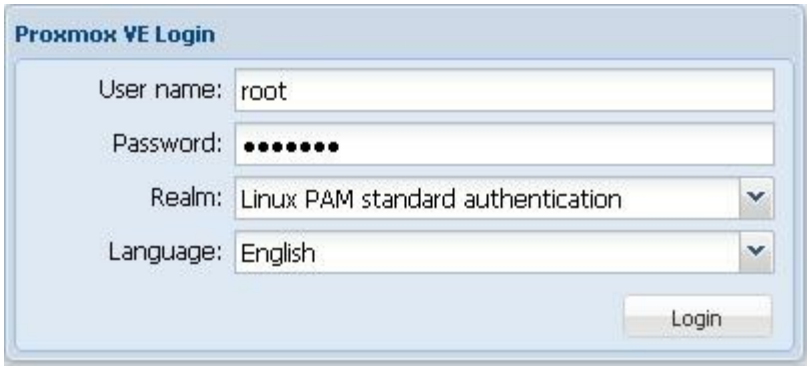
Next: Click ***Add Exception*** as pictured below



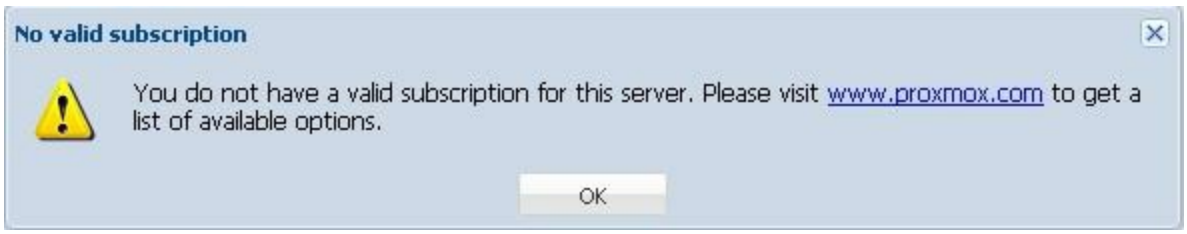
Then: Click ***Confirm Security Exception*** as pictured below



Now login as user: **root** with the password you set during install



Proxmox VE is a community edition but you can elect a subscription account that entitles full support. This is not necessary but you will see the subscription reminder(shown below) each time you log in. I find Proxmox to be an excellent software and really don't mind seeing a popup reminder! After all! It is free!



You will now see the web management interface(shown below). This is where you will create and configure your virtual machines.

PROXMOX Proxmox Virtual Environment
Version: 3.4-1/3f2d890e

You are logged in as 'root@pam' Logout Create VM Create CT

Server View

Datacenter

- Datacenter
  - proxmox5

Search | Summary | Options | Storage | Backup | Users | Groups | Pools | Permissions | Roles | Authentication | HA | Firewall | Support

Search:

Type	Description	Disk usage	Memory usage	CPU usage	Uptime
node	proxmox5	12.5%	35.3%	0.1% of 6CPUs	00:12:50
storage	local (proxmox5)	1.0%			-

Tasks | Cluster log

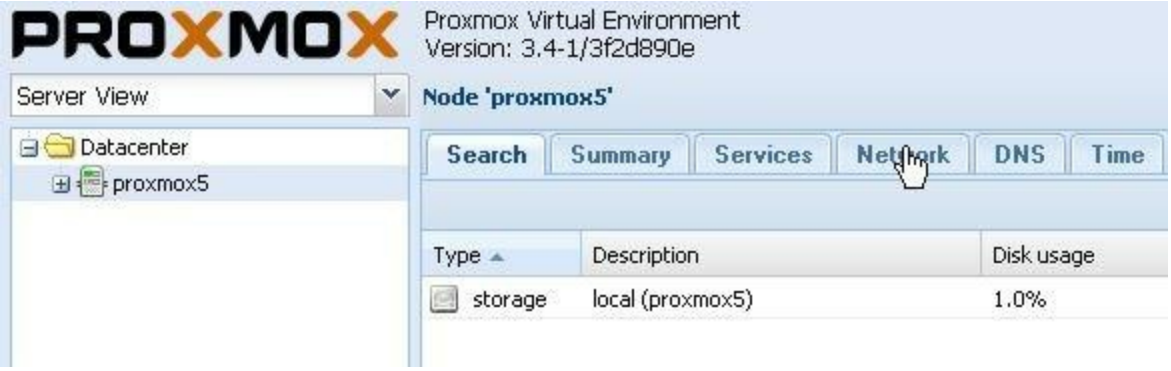
Start Time	End Time	Node	User name	Description	Status
Nov 15 21:59:10	Nov 15 21:59:10	proxmox5	root@pam	Start all VMs and Containers	OK

1.4-Network Adapters

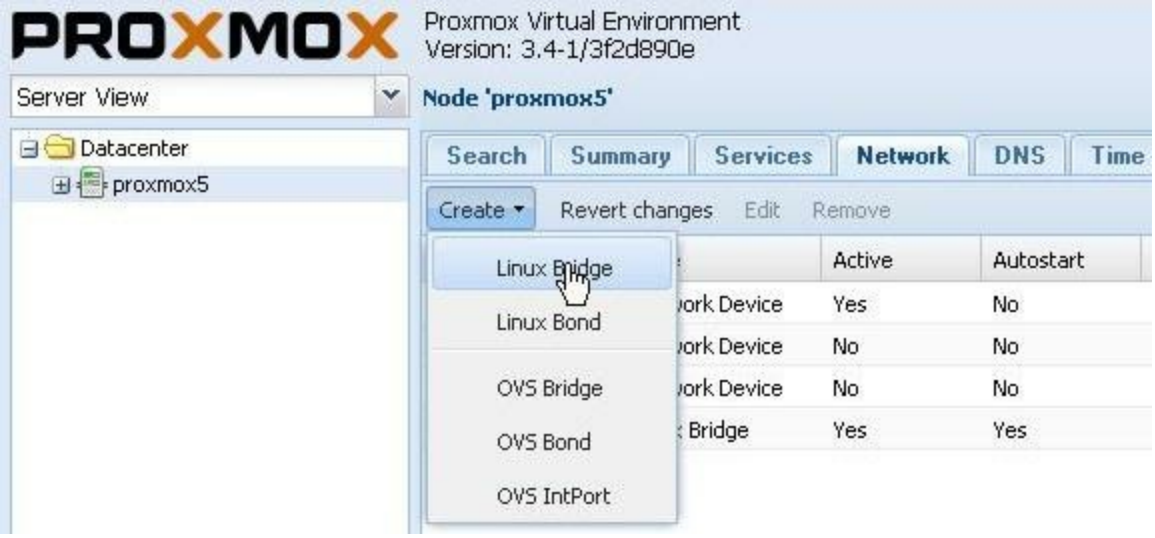
Now you need to configure your network adapters so they can be used for any **VM**'s (virtual machines) you create. Notice that the network tab is not shown in the default view (***datacenter view***). You must be in ***node view*** to see the network tab. In the case pictured below the ***node*** is called **proxmox5**.

Click the node (pictured below)

Click the ***Network tab*** (pictured below)



Click ***Create*** >> ***Linux Bridge*** (pictured below)



You will now see the ***Linux Bridge Dialog*** (pictured below). For each network adapter you will create a bridge. You can see (for this guide) I have filled the form using industry standard naming

convention and have kept a 1:1 relationship between **eth(x)** and **vmbr(x)** ports. For the first time user I would suggest following this rule but you could easily map vmbr1 >> eth2 instead. There will be only 1 default internet **Gateway** which is pre-configured during install and used by **vmbr0** so leave this field blank.

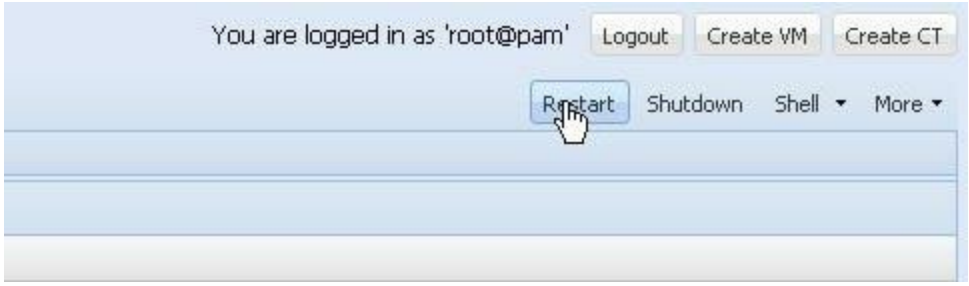
NOTE: For the **IP address** field make sure to use a subnet that will NOT be used in your system (such as 10.10.x.x). Also make sure to use an appropriate **Subnet mask** for your chosen IP address range. IF you are unfamiliar with network addressing Google CIDR for more information. The complexities of network engineering are beyond the scope of this step by step guide but there is a wealth of knowledge to be found on the internet.

When finished click **Create**

NOTE: Repeat the above steps for each adapter you wish to use on your new Proxmox server. For Example: vmbr2 >> eth2 @ 10.10.30.2/255.255.255.0

Changes will not take effect until the system is rebooted.

Restart now using the button in the ***upper right hand corner*** of the node view (you should already be in node view).



When the system finishes rebooting it should refresh the screen automatically. You can **validate** that your virtual interfaces are ready if the **yes** value in the ***active column*** appears(pictured below). Once again, repeat this process for all network adapters you intend to use. You can see here that I have 3 physical adapters but only 2 are configured and ready.

Node 'proxmox5'

Search | Summary | Services | Network | DNS | Time | Syslog | Bootlog | Task History | UBC | Subscription | Firewall

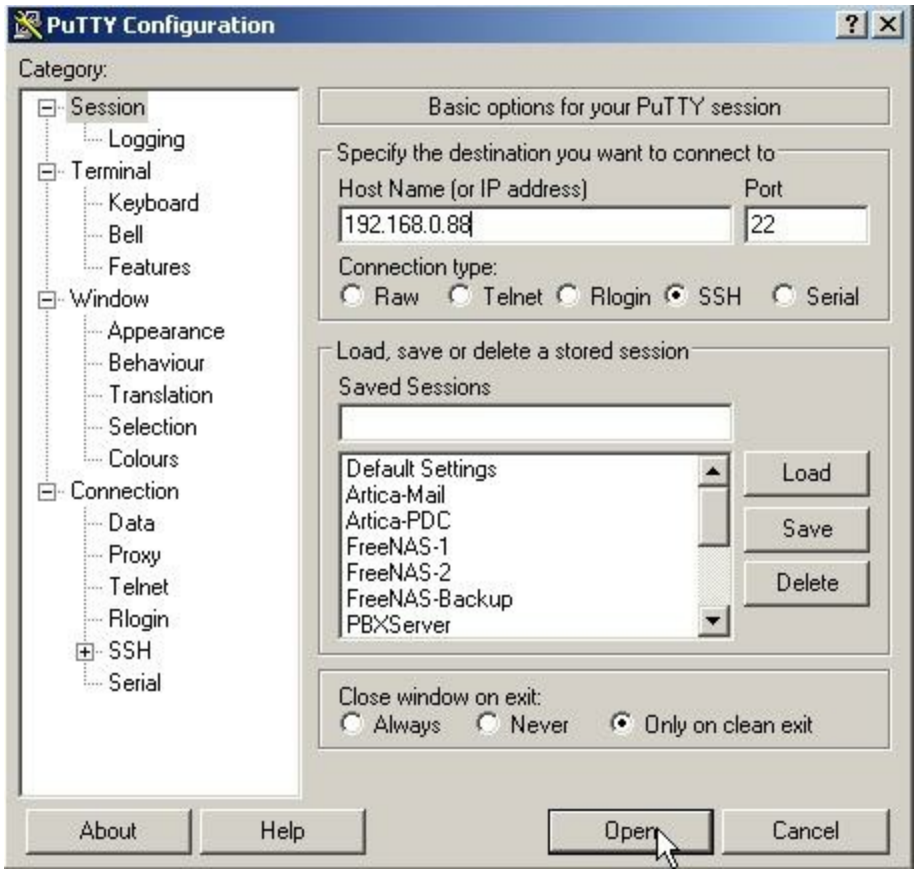
Create ▾ Revert changes Edit Remove

Name ▲	Type	Active	Autostart	Ports/Slaves	IP address	Subnet mask	Gateway
eth0	Network Device	Yes	No				
eth1	Network Device	Yes	No				
eth2	Network Device	No	No				
vmbr0	Linux Bridge	Yes	Yes	eth0	192.168.0.88	255.255.255.0	192.168.0.254
vmbr1	Linux Bridge	Yes	Yes	eth1	10.10.30.1	255.255.255.0	

1.5-Adding LVM Storage

Before you can add **LVM** storage you will need to install **PuTTY**. **PuTTY** is a great open source console which allows **SSH** (Secure shell) access to other computers. It can be downloaded here: PuTTY console

Once installed, open it, check SSH connection, type the ip address of your Proxmox server then click Open.



Click **Yes** to the PuTTY Security Alert (pictured below)

Login as user: **root** with the password you set when installing Proxmox

Now type the following command:

cat /proc/partitions

```
login as:
login as: root
root@192.168.0.88's password:
Linux proxmox5 2.6.32-37-pve #1 SMP Wed Feb 11 10:00:27 CET 2015 x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
root@proxmox5:~# cat /proc/partitions
```

This command will generate a list of hard disk devices as pictured below. We are interested in a new device that does not look to be in service. The **ONLY** possible device as seen below is **/dev/sdb** because it contains no partitions at all. Now we have enough information to setup a ***logical device*** with this disk.

```
root@proxmox5:~# cat /proc/partitions
major minor  #blocks  name

   8       16   83886080 sdb
   8        0   33554432 sda
   8        1       1024 sda1
   8        2     131072 sda2
   8        3   33420288 sda3
 253        0    8126464 dm-0
 253        1    4063232 dm-1
 253        2   17170432 dm-2
root@proxmox5:~#
```

Now that you know which disk to use you can create a ***physical volume*** with the following command:

pvcreate /dev/sdb

```
root@proxmox5:~# cat /proc/partitions
major minor  #blocks  name

   8       16   83886080 sdb
   8        0   33554432 sda
   8        1       1024 sda1
   8        2     131072 sda2
   8        3   33420288 sda3
 253        0    8126464 dm-0
 253        1    4063232 dm-1
 253        2   17170432 dm-2
root@proxmox5:~# pvcreate /dev/sdb
```

You will now see the volume confirmation as pictured below

```
root@proxmox5:~# cat /proc/partitions
major minor  #blocks  name

   8       16   83886080 sdb
   8        0   33554432 sda
   8        1       1024 sda1
   8        2     131072 sda2
   8        3   33420288 sda3
 253        0    8126464 dm-0
 253        1    4063232 dm-1
 253        2   17170432 dm-2
root@proxmox5:~# pvcreate /dev/sdb
  Physical volume "/dev/sdb" successfully created
root@proxmox5:~#
```

Now that a ***physical volume*** exist you can create a ***volume group*** called lvstorage (or some other name of your choice).

To create the ***volume group*** issue the following command:

vgcreate lvstorage /dev/sdb

```
root@proxmox5:~# cat /proc/partitions
major minor  #blocks  name

   8       16   83886080 sdb
   8        0   33554432 sda
   8        1       1024 sda1
   8        2     131072 sda2
   8        3   33420288 sda3
 253        0    8126464 dm-0
 253        1    4063232 dm-1
 253        2   17170432 dm-2
root@proxmox5:~# pvcreate /dev/sdb
  Physical volume "/dev/sdb" successfully created
root@proxmox5:~# vgcreate lvstorage /dev/sdb
```

You will now see the ***volume group*** confirmation as pictured below

```
   8       16   83886080 sdb
   8        0   33554432 sda
   8        1       1024 sda1
   8        2     131072 sda2
   8        3   33420288 sda3
 253        0    8126464 dm-0
 253        1    4063232 dm-1
 253        2   17170432 dm-2
root@proxmox5:~# pvcreate /dev/sdb
  Physical volume "/dev/sdb" successfully created
root@proxmox5:~# vgcreate lvstorage /dev/sdb
  Volume group "lvstorage" successfully created
root@proxmox5:~#
```

You are now finished in the command console and may close the **PuTTY** program.

I highly recommend learning as much about Linux **LVM** as possible. It is my preference to use **LVM** for everything! It boots using **UUID serialization** which makes it bullet-proof-bootable and allows for easy removal of drives for relocation to other machines. You can also create ***striping*** or ***mirrored*** volumes and it supports snapshots, resizing, moving, etc.... It is light weight and fits our

simplicity model perfectly!

About LMV

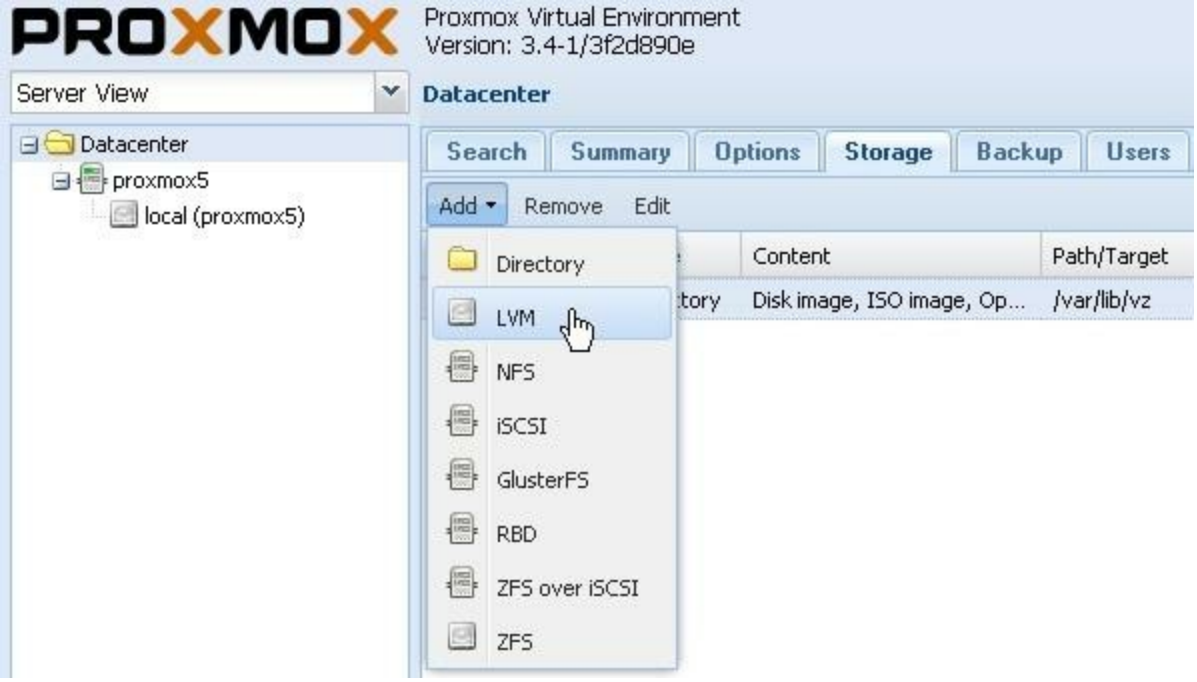
LVM storage is characterized by three components, which are, physical volumes, volume groups, and logical volumes. A volume group is made up of 1 or more physical volumes. A PV (physical volume) is nothing more than a hard drive. The primary storage component is the logical volume. A volume group can be sliced up into many logical volumes. For example: You have 3 x 500GB physical disks making up your VG (volume group). These are /dev/sda,b,and c respectively. The total capacity of this group will be 1.5TB which you may name vg_500gbint. I like to use a name that tells what device sizes I am using and whether they are internal or external devices. You could then create 2 x 750GB LV's (logical volumes) or 15 x 100GB LV's from your 1.5TB VG.

You may wish to name your LV's something like lv1_vg500gbint indicating it as the first logical volume associated with the volume group named vg_500gbint.

1.6-Configure LVM Storage

Now that you have added a logical volume group at the command line it is time to configure how it is used in Proxmox. One thing to note is that(in this guide) LVM storage through the web interface will only be used for VM images. This special storage area is where all your virtual machines will keep their assigned hard drives.

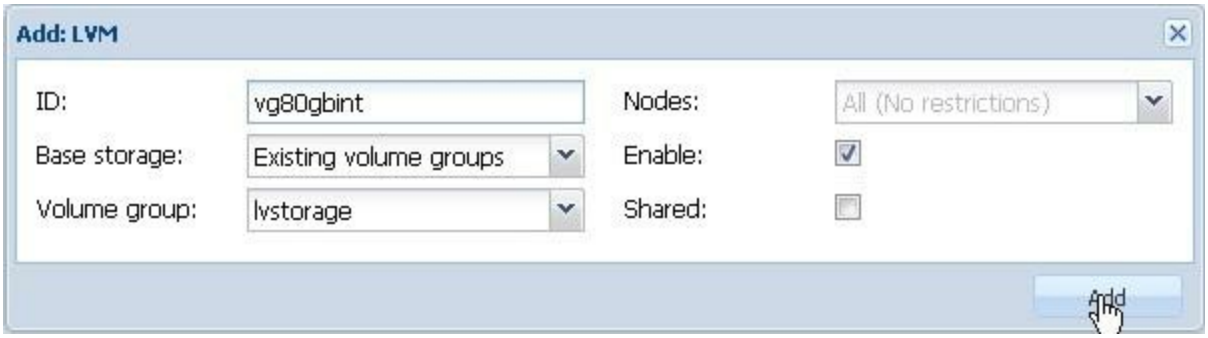
To get started make sure your in datacenter view then click the Storage tab(pictured below). Next click **Add** >> **LVM**(pictured below).



You should now see the LVM dialog box(pictured below). The **lvstorage group** you created using PuTTY can now be selected. Type a unique name for the **ID** field(pictured below).

When finished: Click **Add**.

NOTE: Often times I choose a name that indicates the storage type such as **LV_vg80gbint**.



You should now see your new LVM storage in the tree view(pictured below). Clicking on the summary tab shows the available size of your new storage(pictured below).

PROXMOX Proxmox Virtual Environment
Version: 3.4-1/3f2d890e

Server View

Storage 'vg80gbint' on node 'proxmox5'

- Datacenter
  - proxmox5
    - local (proxmox5)
    - vg80gbint (proxmox5)

Summary | Content | Permissions

Status	
Enabled	Yes
Active	Yes
Content	Disk image
Type	LVM
Shared	No
Size	80.00GB
Used	0
Avail	80.00GB

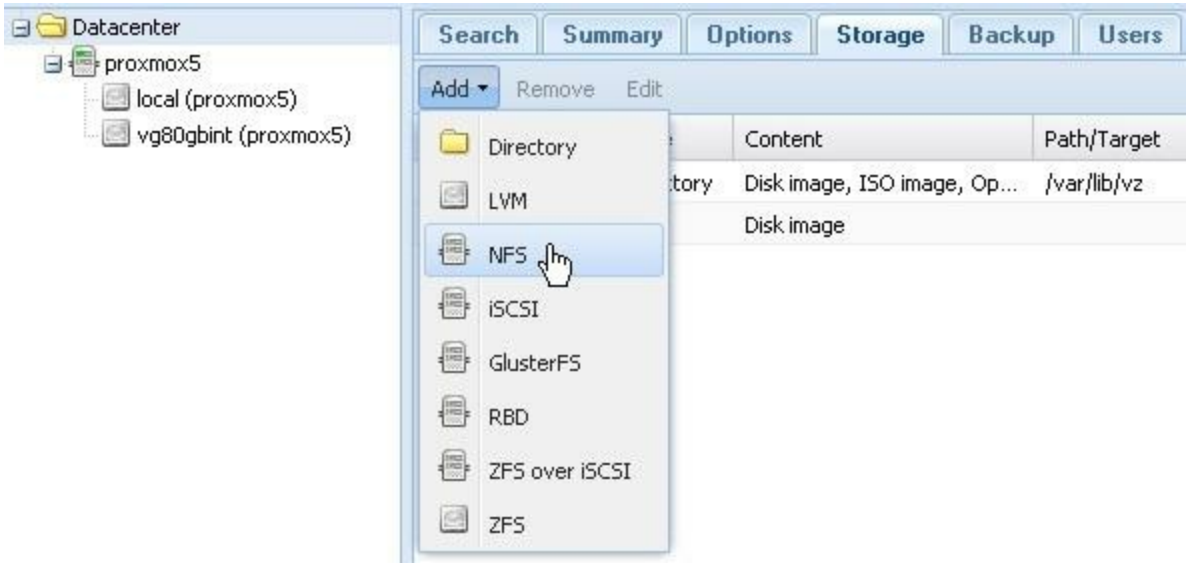
1.7-Configure NFS Storage

NFS is perhaps the most diverse of all storage types you will use. It is a network based storage so you will need a NAS configured on your local subnet in order to use it. NFS can be used for image, backup, template, ISO, and container storage in Proxmox. I have extensively tested all types of storage in Proxmox over the years. As previously mentioned, my storage of choice for local images is LVM based! Well, my preference for network backed storage is NFS! It offers performance rivaling that of iSCSI without any of the complexities.

In this section I will demonstrate the configuration of an existing NFS share to be used for VM backup archives. In production you will probably want(at least) an additional share for CD/DVD ISO files. Backups and ISO's are the ones I tend to need the most!

To get started make sure your in datacenter view then click the Storage tab(pictured below).

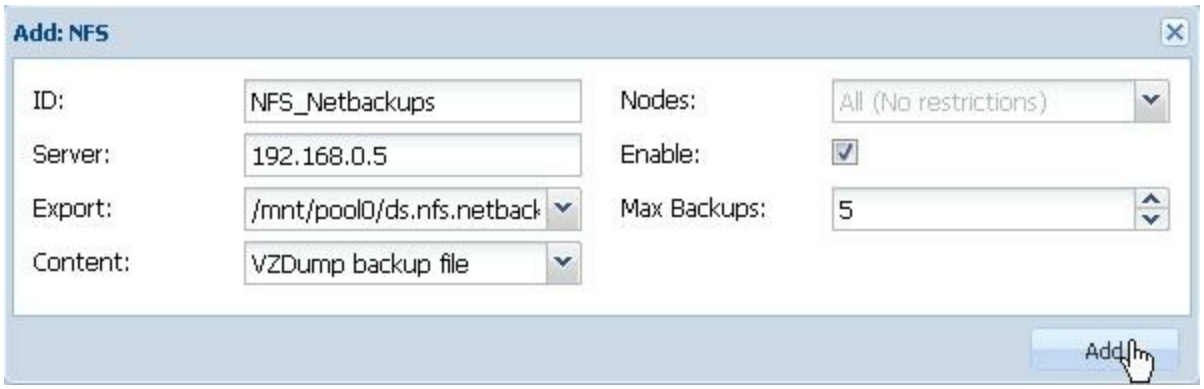
Next click **Add** >> **NFS**(pictured below).



You should now see the NFS dialog box(pictured below). Type the IP address of your NAS storage. Type a unique name for the **ID** field(pictured below). Choose the appropriate NFS Export from the dropdown list. You can also select how many backup archives are allowed per VM.

When finished: click **Add**.

NOTE: Often times I choose a name that indicates the storage type such as **NFS_NetBackups**.



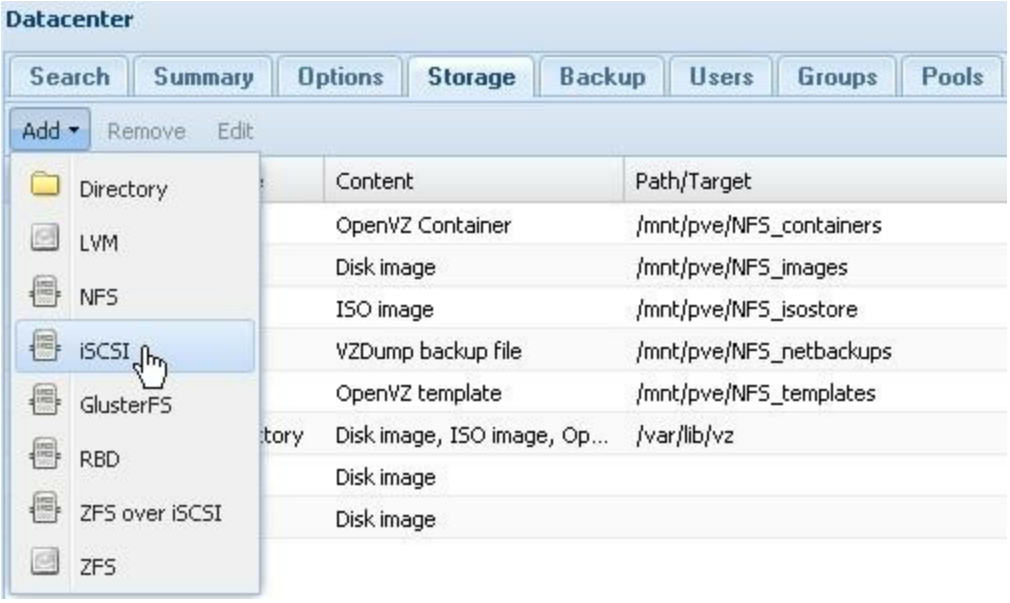
You should now see your new NFS storage in the tree view(pictured below).

1.8-Configure iSCSI Storage

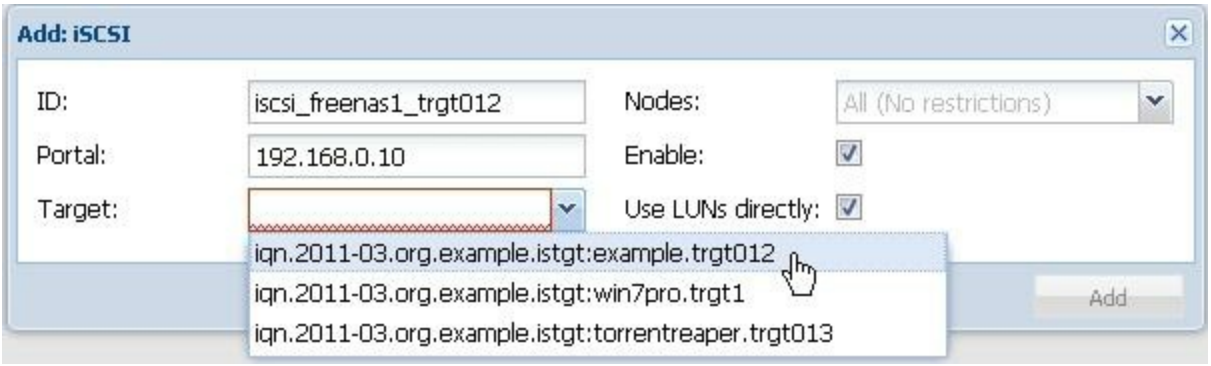
The 3rd and final storage option for Proxmox that we will cover in this book is **iSCSI**. This storage type is typically used by large enterprise with hundreds of servers where internet speed is the limiting factor and intermittent performance dynamics are expected. Because it is ***network backed storage***, VM performance suffers compared to dedicated hardware installs. For this reason I do not recommend using it for any critical production application.

Although it does have network imposed limitations it is very flexible and when used with high quality hardware can yield very reasonable performance. Where iSCSI shines is in a large testing environment where you need temporary storage space allocations on a frequent basis. Because it fools the operating system into thinking it has extra local disks the possibilities are endless. For example: It could easily be used to configure an LVM based mirrored array that is mapped to a specific directory then mounted and used for VM images, containers, templates, etc. To learn how iSCSI targets are setup in freeNAS click here: 3.16.3-iSCSI Target Shares

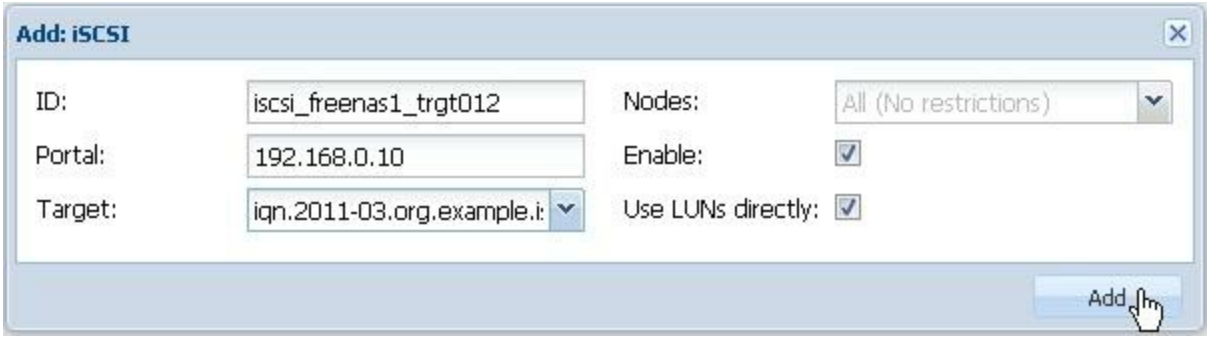
To map an iSCSI target make sure your in **Datacenter >>Storage** then click **Add>>iSCSI**(shown below).



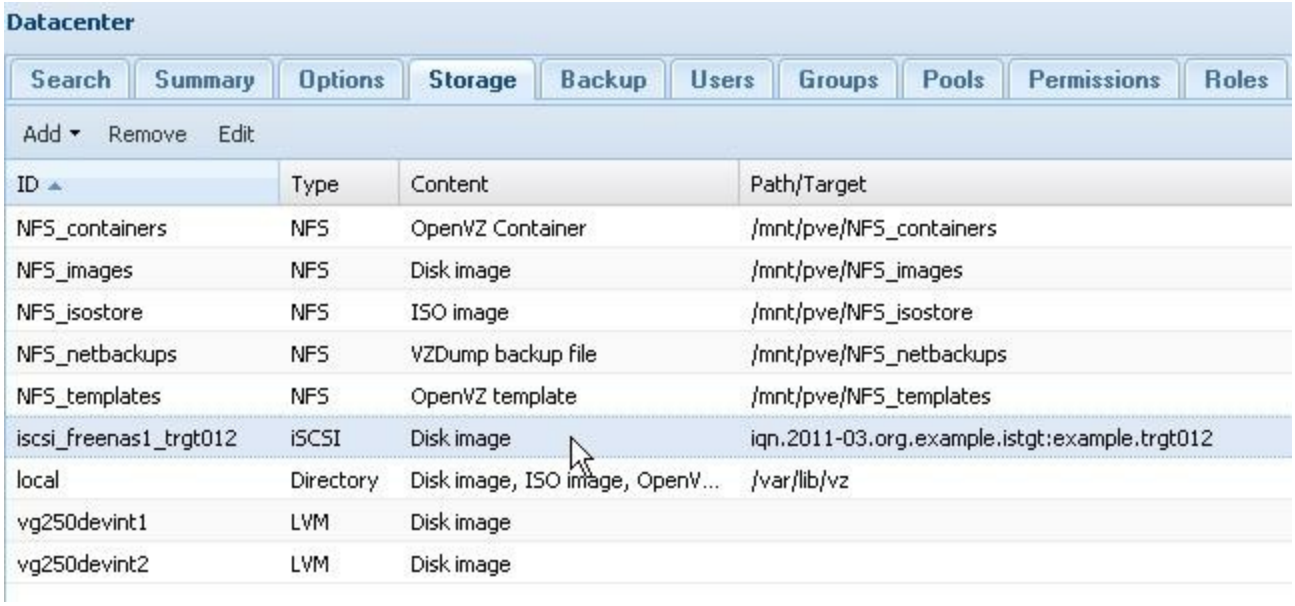
You will then see the following dialog. Enter the **ID** and **Portal** information then select the **Target** from the dropdown list(shown below). If you ***do not*** wish to configure the target as an ***LVM disk*** for ***mounting*** make sure the option **Use LUN's directly** is checked.



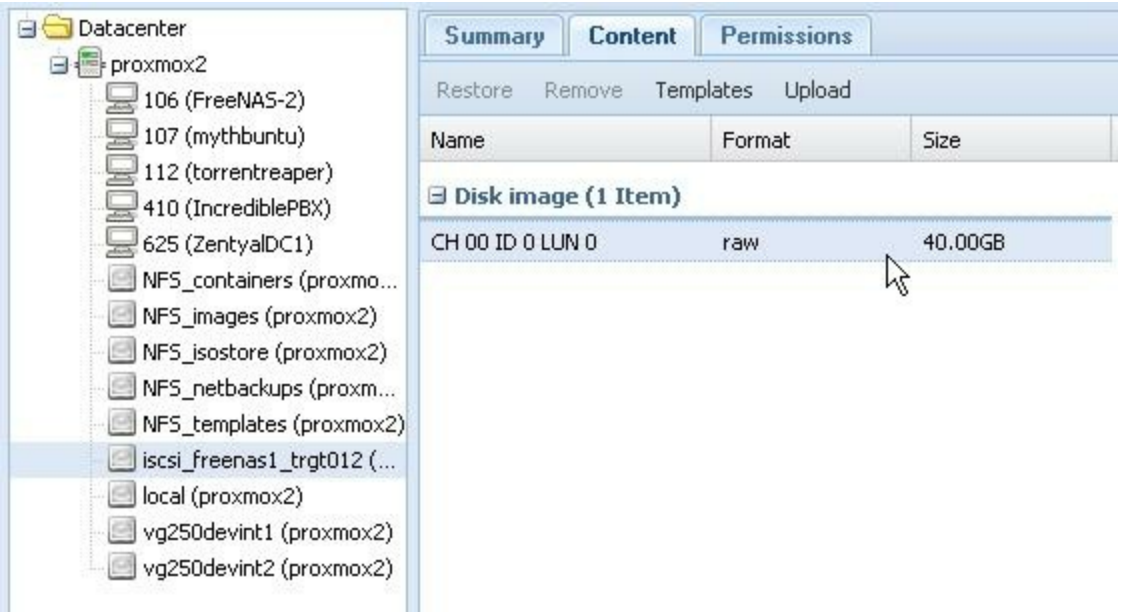
To proceed: click the **Add** button(shown below).



When the target has been successfully added it will appear as a new storage device(pictured below).



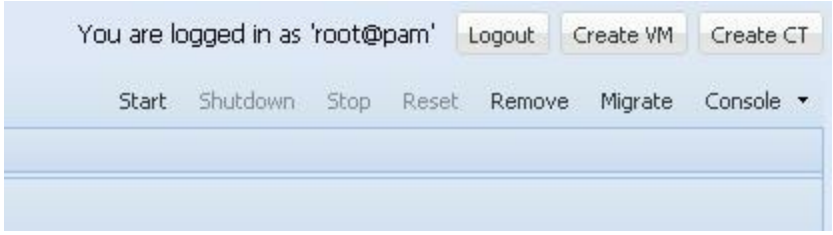
You should now be able to view the content information by selecting it from the node tree(shown below).



1.9-Creating VM Configurations

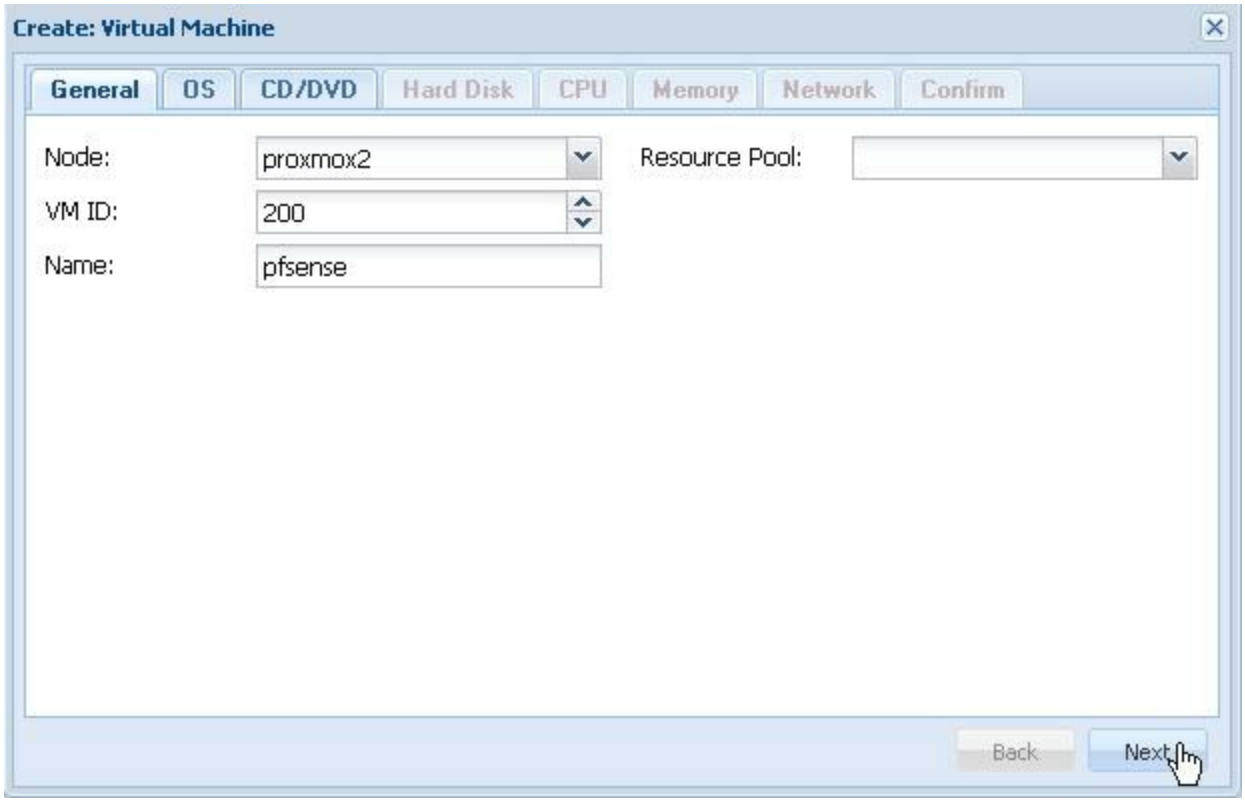
Now that you have Proxmox configured you can create your first VM(virtual machine)! Let's get a pfSense router configuration setup!

To begin: click **Create VM** in the upper right corner.



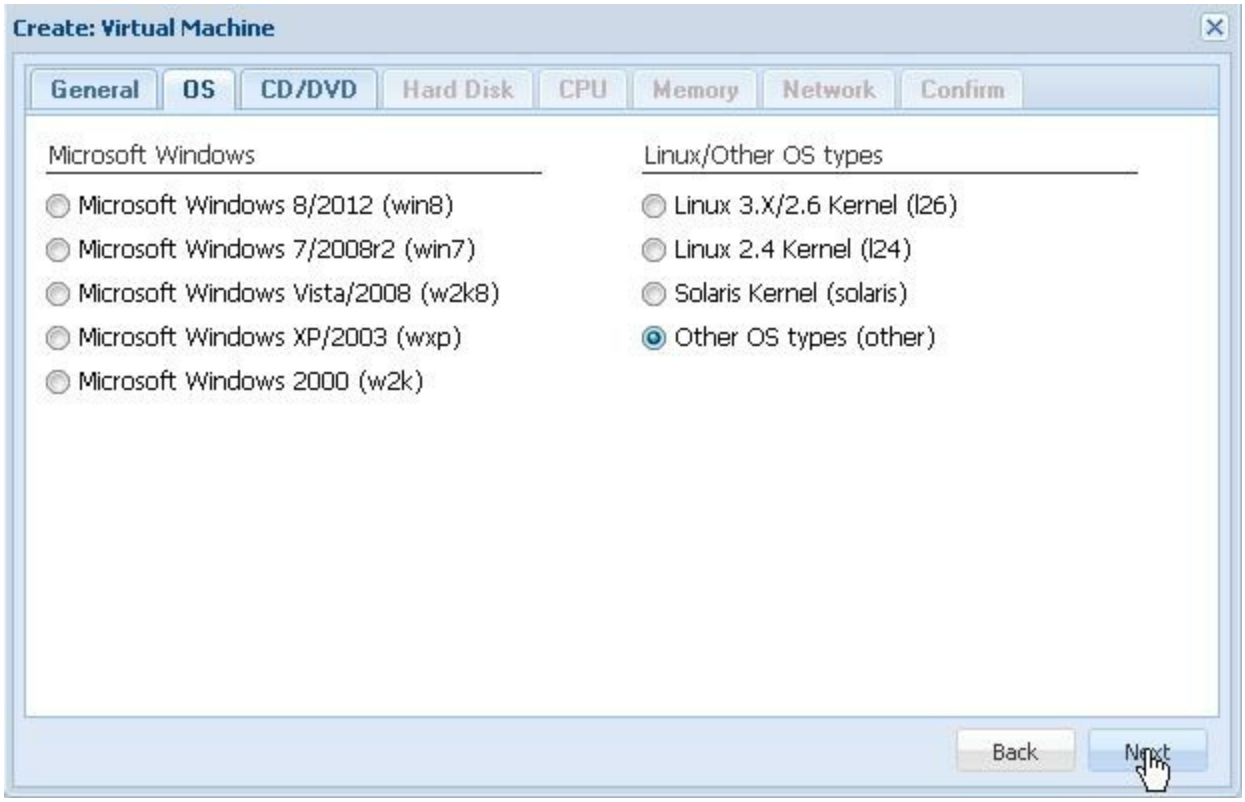
Now assign an **ID** and **Name** your new VM.

To continue: Click **Next**



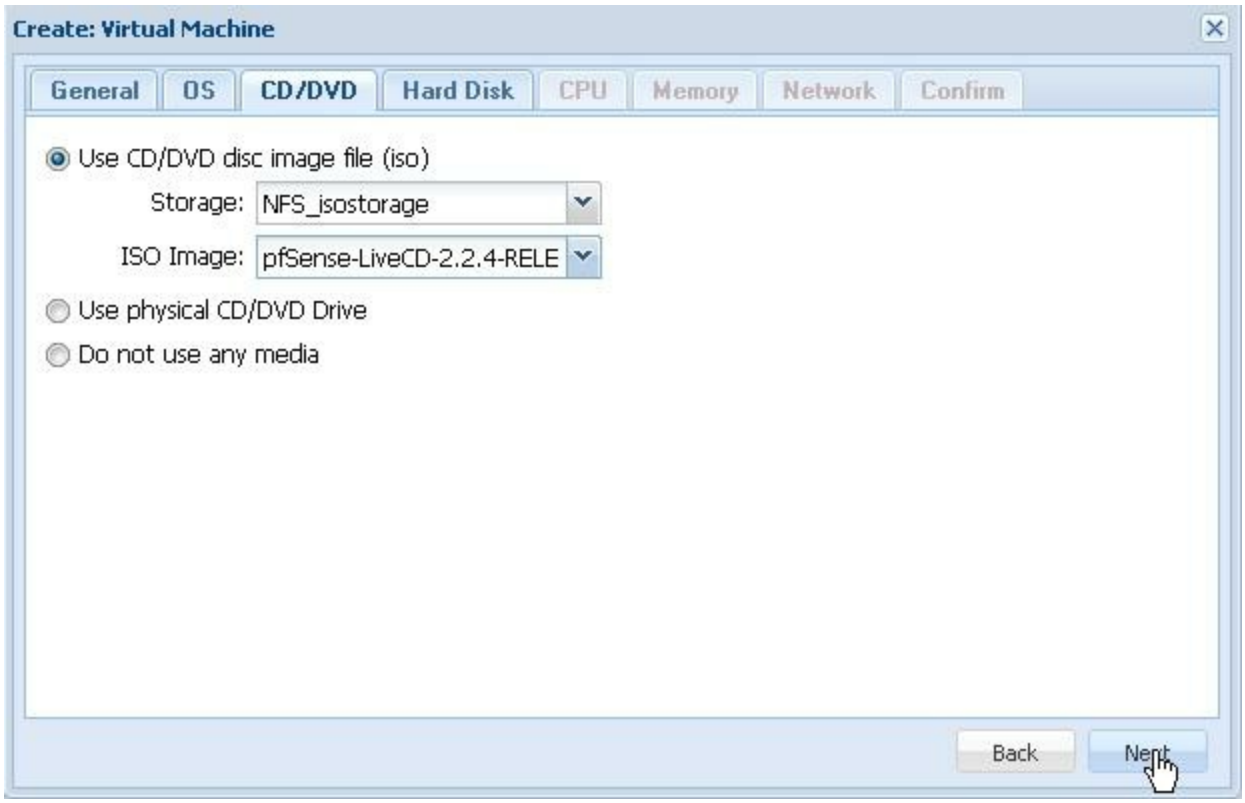
Next, select the OS type. pfSense is BSD based so choose (other).

To continue: Click **Next**



The next step assumes that you have an ISO storage setup and working with the latest pfSense-LiveCD. For this guide I am using version 2.2.4 Release. If you don't have any ISO storage you can click local in the node tree view then upload your CD/DVD image. Alternatively, you can burn the ISO to disk then select Use physical CD/DVD Drive(pictured below).

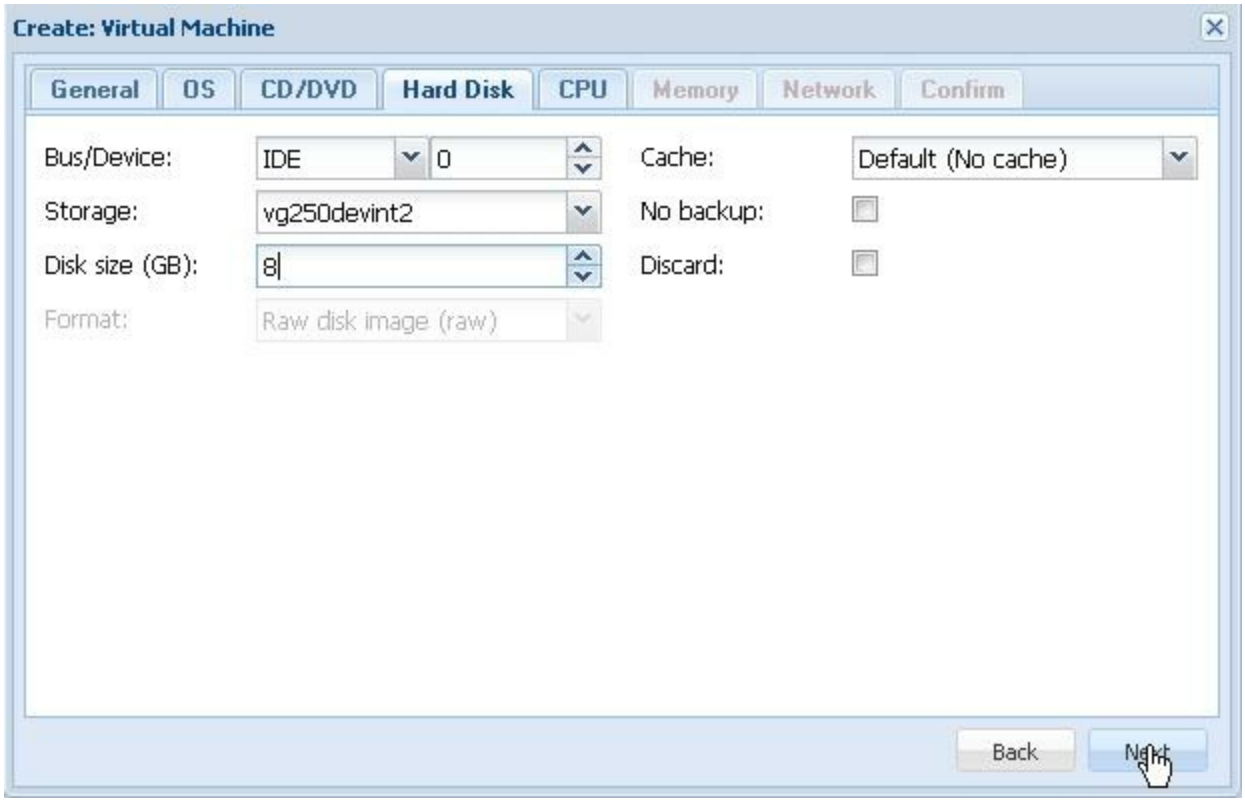
To continue: Click **Next**



Next, you will configure hard disk parameters. For this pfSense install use IDE device type with 8GB disk. You can choose local or the lvstorage you configured earlier in this guide.

NOTE: After extensive testing my preferred disk configuration is ALWAYS to use IDE Bus, Raw disk Format, and Default Cache settings.

When finished: Click **Next**

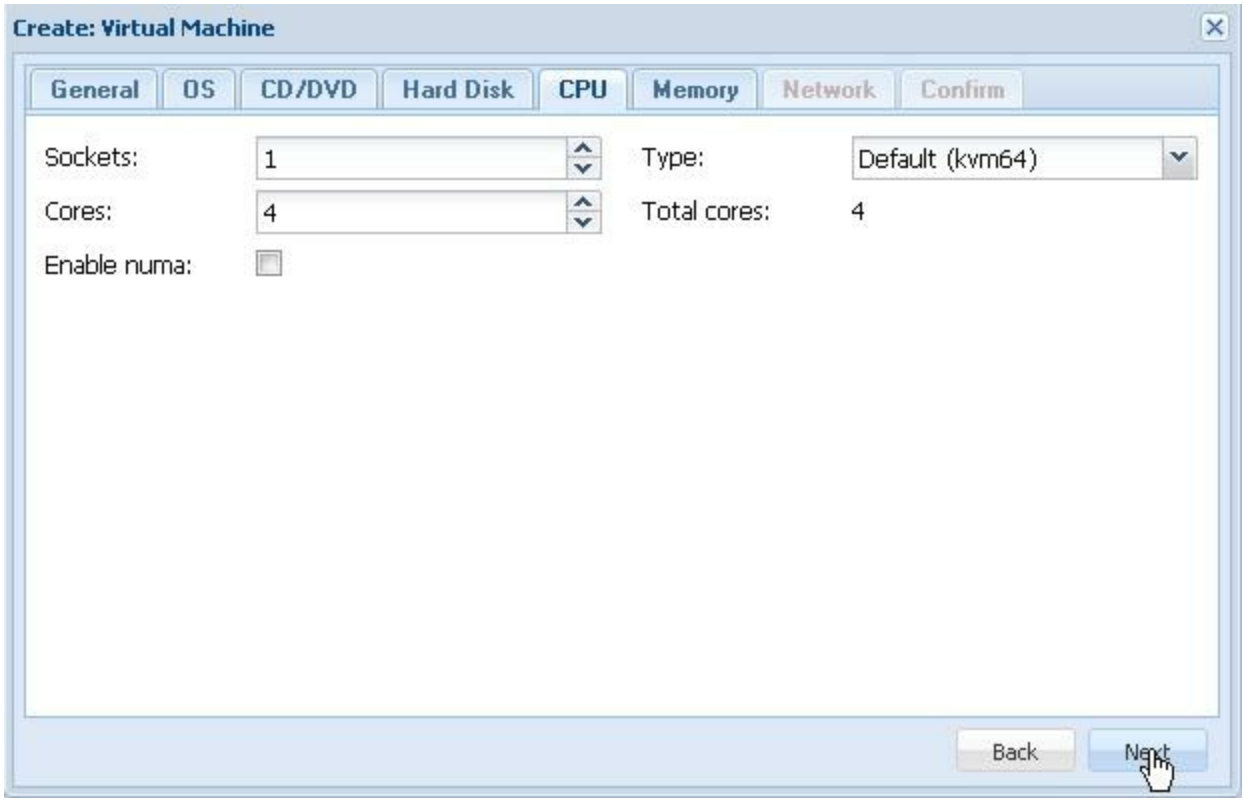


Now select how many CPU cores to use for processing. Do NOT set more cores than you have available or your VM will not boot! For CPU type I recommend KVM. In some cases your VM may fail to boot. If that's the case select QEMU instead.

SPECIAL CASE: The BSD based pfSense is one of those cases where you MUST select a QEMU CPU type.

NOTE: If your VM won't boot it can usually be traced back to an improper CPU type. Also, you will usually select 64 bit unless you have a 32 bit need.

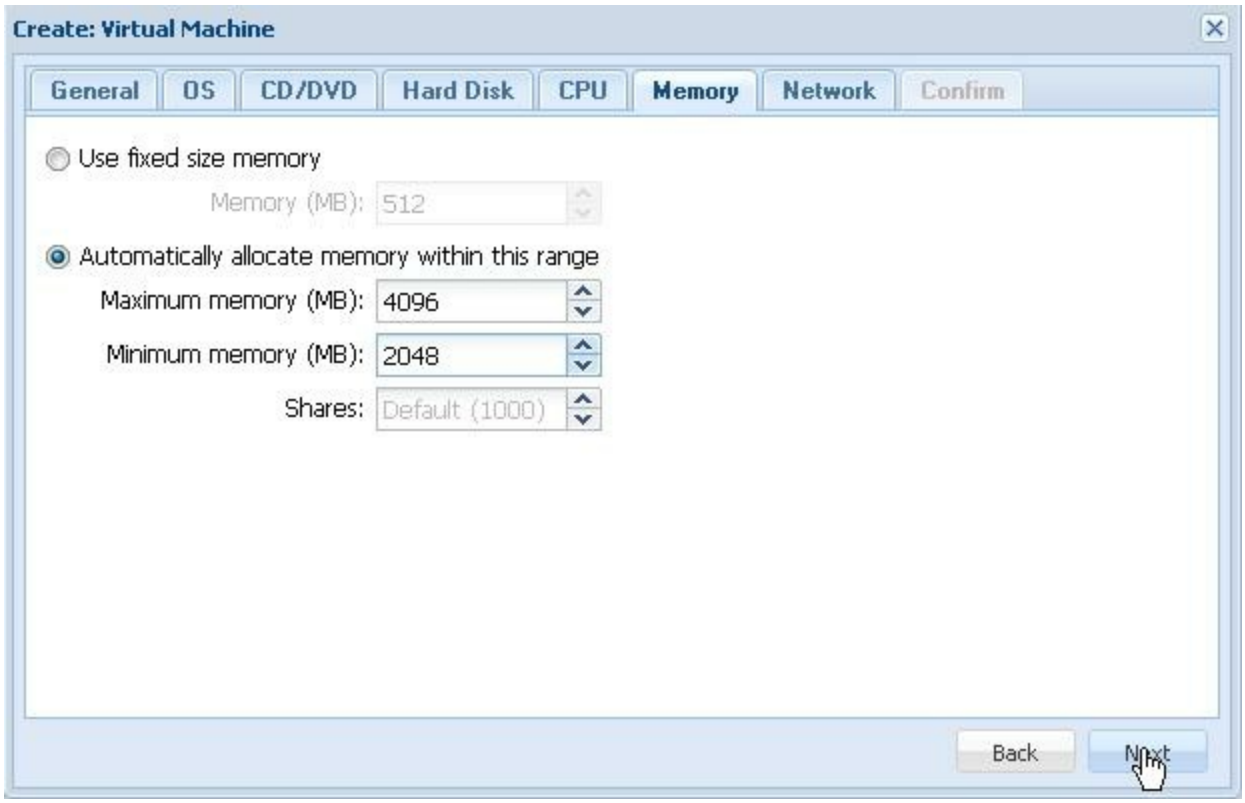
When finished: Click **Next**



You will now need to configure memory. The two modes are fixed and auto. I tend to use auto the most because it shares memory and will NOT allow over-allocation. I suggest running pfSense with the memory configuration as shown below.

NOTE: It is possible to assign so much fixed memory that the Proxmox OS is deprived of memory resource!

To continue: Click **Next**

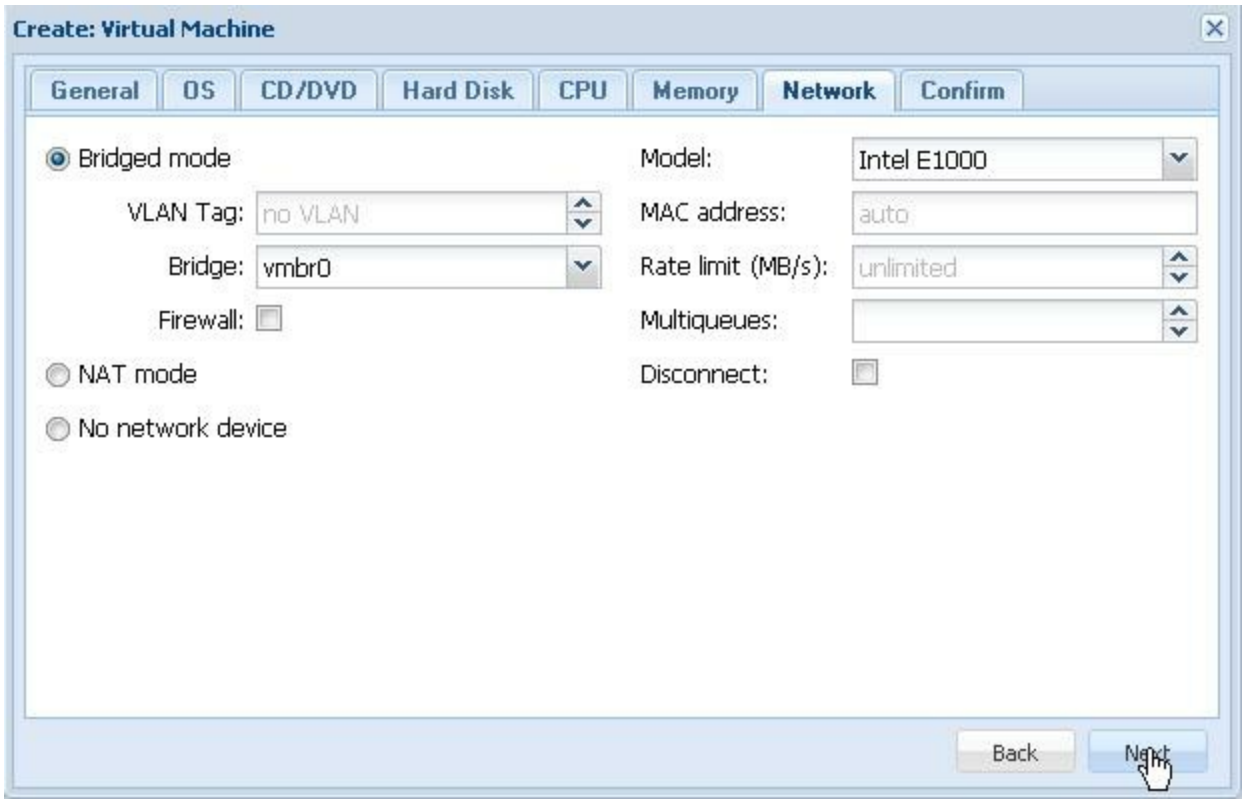


Next you will setup the network bridge. We will set the pfSense LAN adapter to vmbr0. This is safe

with a router because the only traffic passing through is internet, which is low bandwidth relative to the network adapters maximum capacity. For adapter model select Intel E1000. I strongly recommend it!

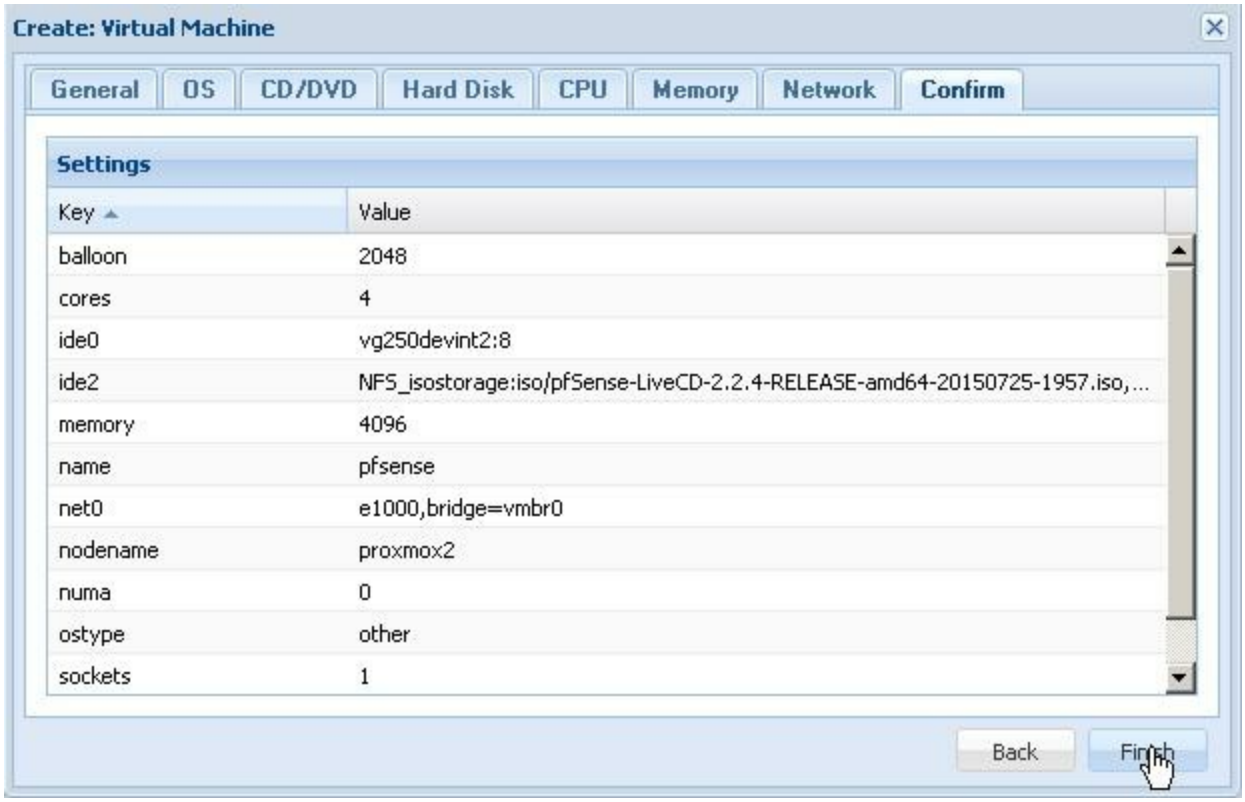
NOTE: Normally you will NOT want to use vmbr0 for VM's because it is the default adapter for the user interface! You can use it! Just try to avoid doing so unless the VM is low bandwidth.

To continue: Click **Next**



Finally you will confirm the configuration.

To continue: Click **Finish**

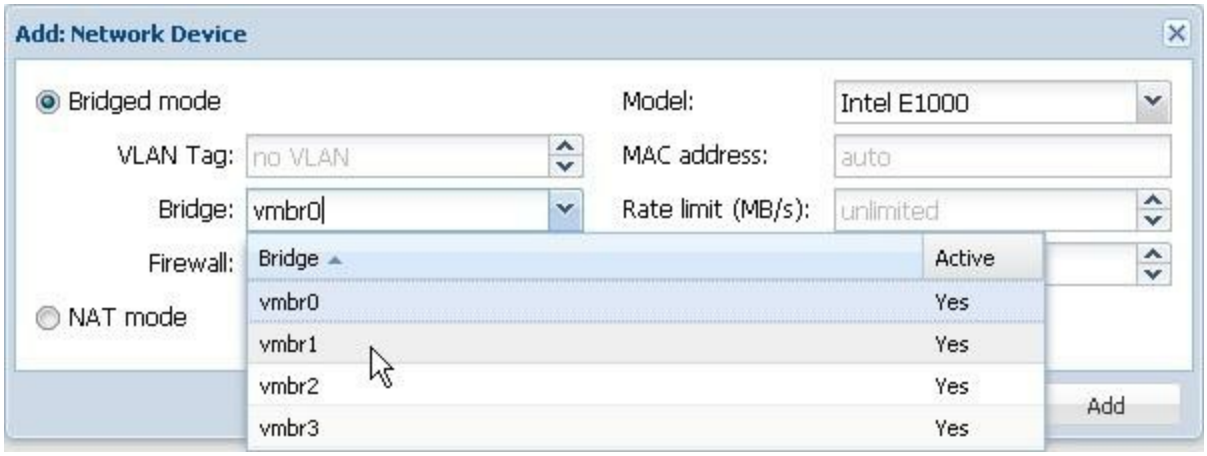


At this point you should be able to see your new VM configuration in the node tree as pictured below. You can click the various tabs at the top for additional configuration options. You can also edit individual items within the configuration by clicking on them and selecting edit

Since your pfSense router only has one network adapter we will need to add another. The new adapter is needed for your WAN(Internet) connection. It is important that you know the correct Mac/Hardware address for this to work. If you followed the directions to this point you should have labeled the adapters making it easy to match the Mac/Hardware addresses by looking at the back of the machine.

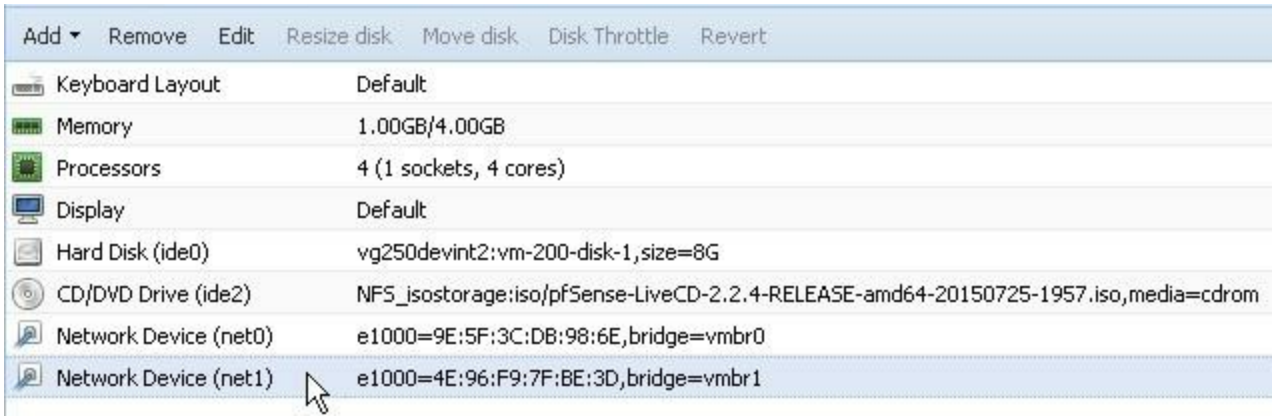
Let's continue: Click **Add** >> **Network Device**

Now add a new network bridge(shown below). For this example I have chosen vmbr1 but that can be changed very easily whenever you want.



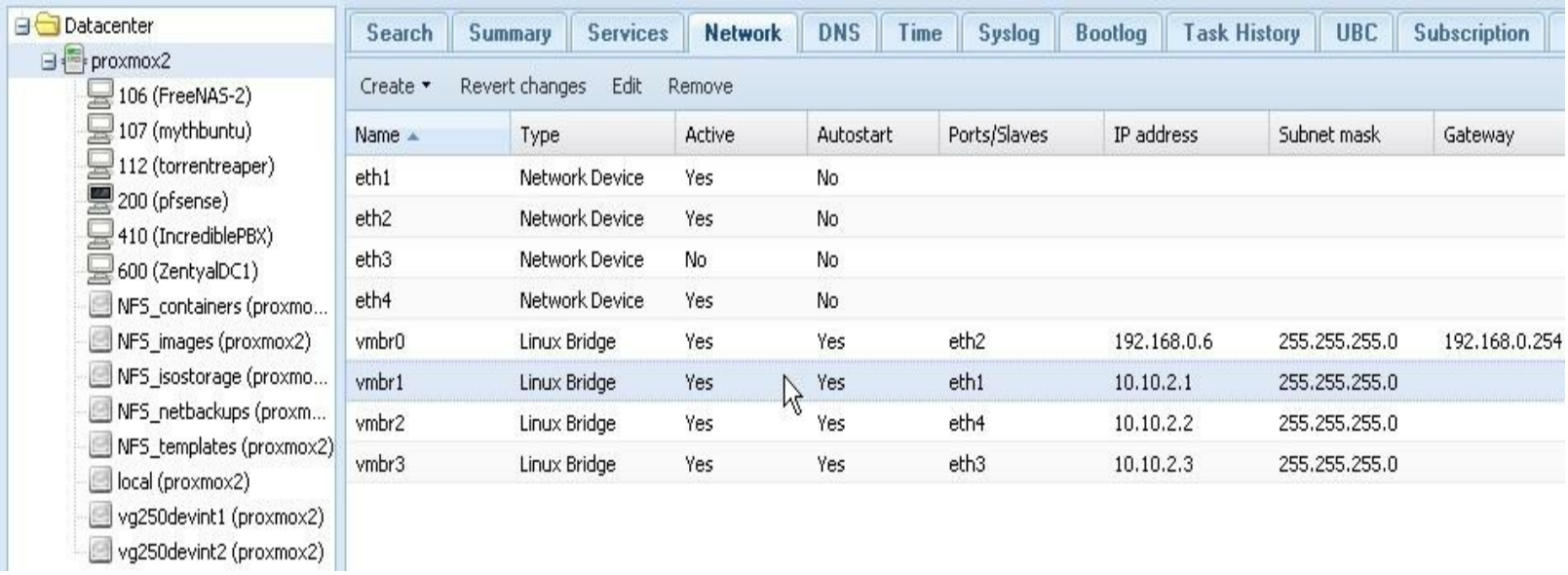
Now you will see your newly added adapter in the hardware list(pictured below).

MAC address NOTE: The hardware address you see is an alias and not the actual hardware address! That's why you labeled them!



Now let's double check the association between vmbr1 and eth1. We just want to make certain that vmbr1 doesn't point to eth4 instead. To check the association go to the network tab in node view(pictured below). You can clearly see associations between all the adapters. We still don't

know the real Mac address though!



Name	Type	Active	Autostart	Ports/Slaves	IP address	Subnet mask	Gateway
eth1	Network Device	Yes	No				
eth2	Network Device	Yes	No				
eth3	Network Device	No	No				
eth4	Network Device	Yes	No				
vmbr0	Linux Bridge	Yes	Yes	eth2	192.168.0.6	255.255.255.0	192.168.0.254
vmbr1	Linux Bridge	Yes	Yes	eth1	10.10.2.1	255.255.255.0	
vmbr2	Linux Bridge	Yes	Yes	eth4	10.10.2.2	255.255.255.0	
vmbr3	Linux Bridge	Yes	Yes	eth3	10.10.2.3	255.255.255.0	

To find out which adapter to plug your internet into will require an additional step. I know this may seem complicated but it's really not that bad once you wrap your head around it. You will use a special Linux command called **ifconfig**.

ifconfig eth1

Let's find that Mac now!

Open up your PuTTY program and login as root like you did when we setup the storage.

Now type the command below followed by the Enter key.

ifconfig eth1

The results will show the actual Mac/Hardware address as picture below.

```
login as: root
root@192.168.0.6's password:
Linux proxmox2 2.6.32-37-pve #1 SMP Wed Feb 11 10:00:27 CET 2015 x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Fri Sep  4 00:40:11 2015 from win7pro.linuxsolutions.us
root@proxmox2:~# ifconfig eth1
eth1      Link encap:Ethernet  HWaddr 00:14:d1:23:38:a8
          inet6 addr: fe80::214:d1ff:fe23:38a8/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:50044688 errors:0 dropped:0 overruns:0 frame:0
          TX packets:19729662 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:29952488501 (27.8 GiB)  TX bytes:2177534122 (2.0 GiB)

root@proxmox2:~#
```

Now that you have the real HW address you can match the labeled adapter and plug in your internet.

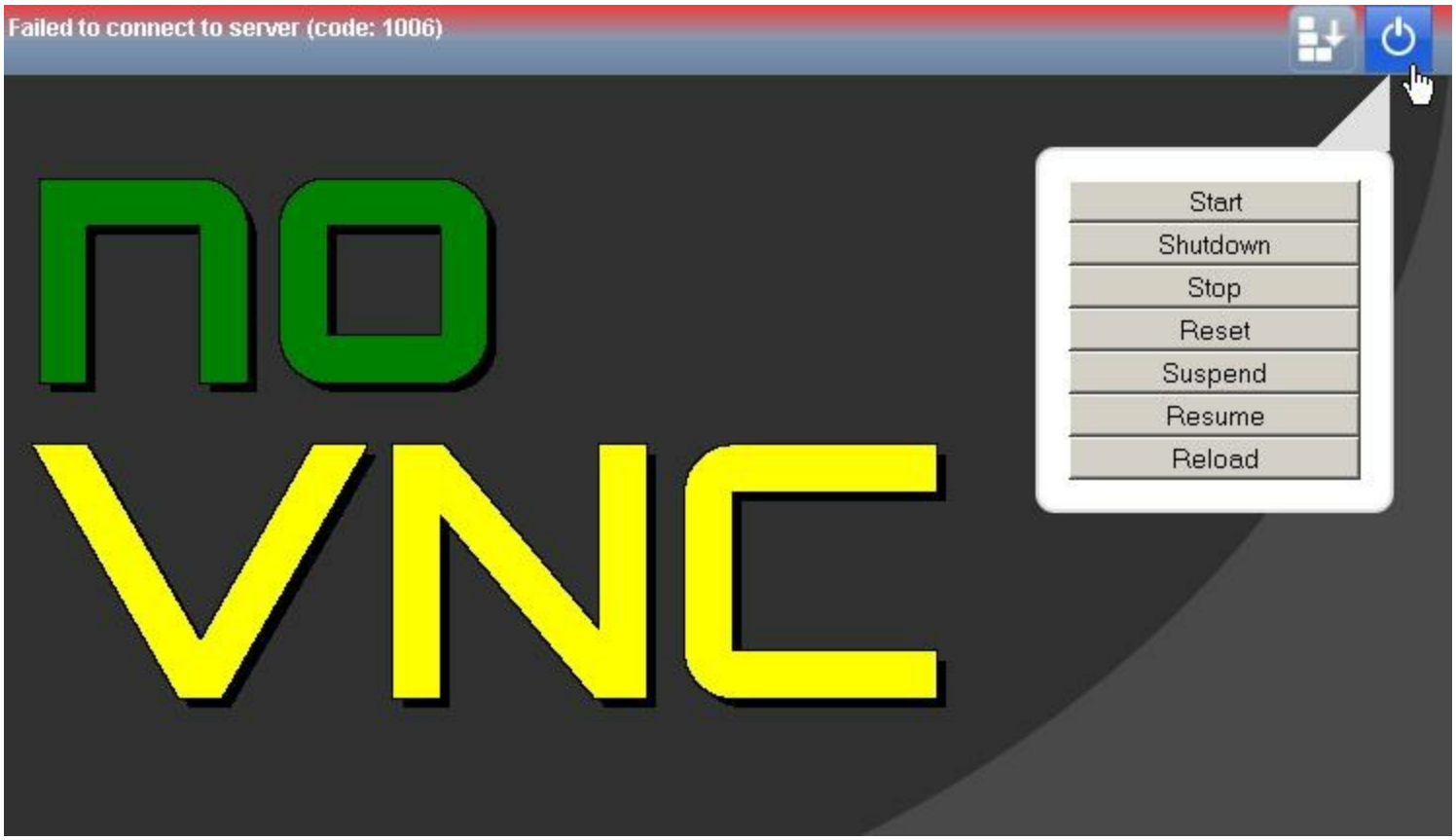
NOTE: Because of this special Mac matching requirement for the WAN ports you won't be able to share these adapters with other VM's . The solution is in planning which Proxmox servers will be used for router instances then add extra network adapters to only those machines. That's a small price to pay for the ability to easily move your internet gateway.

It's also possible to use a small 5 port switch to allow offline migration of your routing gateway. Just select another Proxmox server you want to use for a pfSense cold copy(off-state), repeat the address matching procedure on that machine, and plug into the 5 port switch along with your live pfSense and your incoming internet.

In summary: your incoming internet connection plugs into the 5 port switch and each pfSense VM WAN port also plugs into that switch. Please see (Option-3) Easy Offline Router Migration for more information.

DMZ and WAN2: I don't suggest installing these extra adapters until after the initial pfSense installation is completed. You will need at least one more virtual adapter for DMZ if following this complete guide. When that time comes just refer back to this section and repeat the process for adding a new network adapter.

Now that your configuration is complete you need to know how to boot it. Simply select the VM in the node tree and click the start button in the upper right hand corner. Alternatively, if installing an OS you may wish to select the console so you can respond to prompts. Just click the start option in the console(pictured below). Once your VM starts up it will look like any other operating system booting. To follow the install of pfSense click here: Book 2: pfSense



1.10-VM Backup & Restore

Please take advantage of the following information as mentioned earlier in .3-Best Practices**.**

Disaster Recovery Simplified

If any of your Proxmox servers go down the single most important item to recover will **ALWAYS** be your ***VM image backups***. Think of them as Master Recovery Images! Without these you are lost so it is important to have as many copies as possible!

My preferred method is to select a NAS(virtualized or standalone) to use as my **primary *VM image backup* server**. This server will host the NFS image backup share to Proxmox. This share is manually replicated(only once during setup) to all other NAS servers in the system and synchronized on schedule using Rsync.

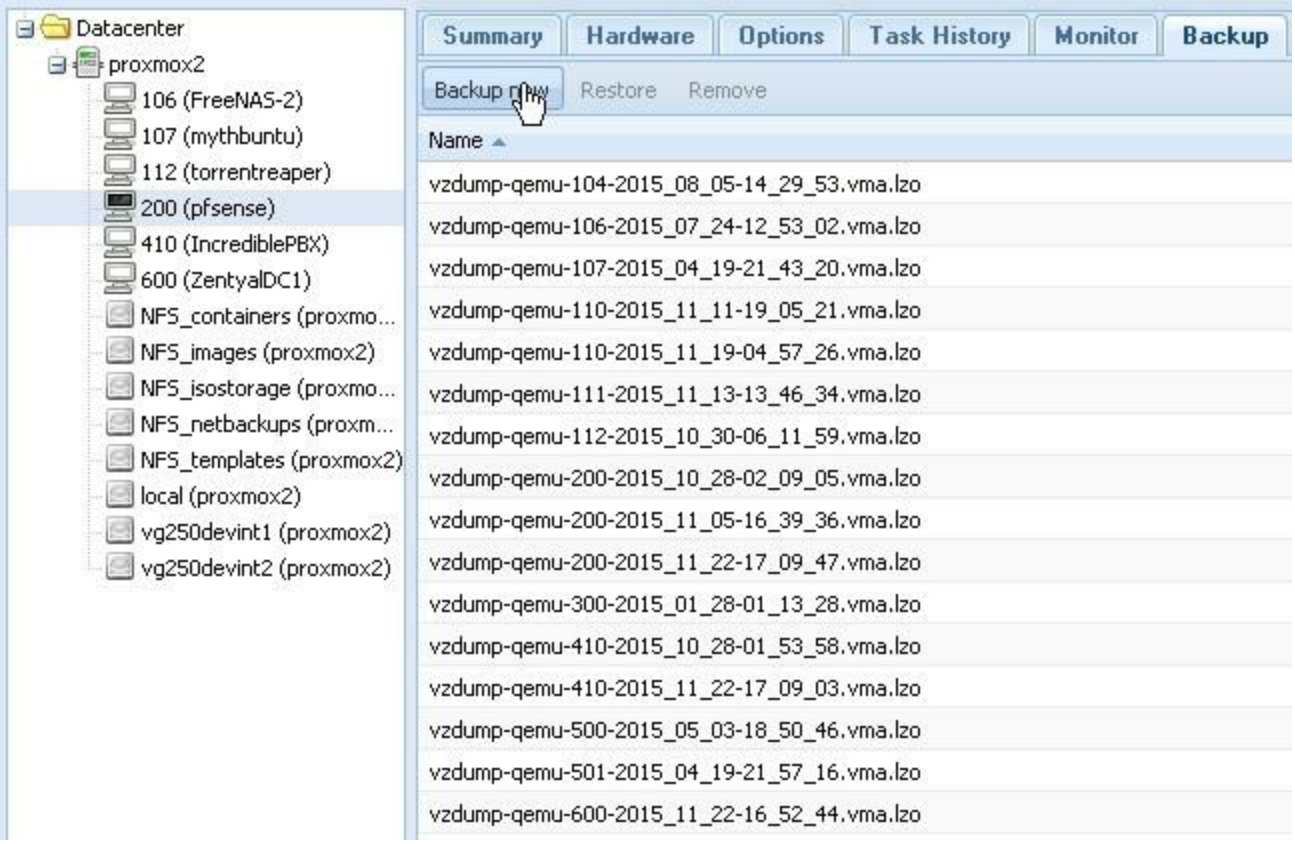
If a machine goes down I can replace it, re-install Proxmox, re-install any NAS drives , re-map my NFS backups, and restore the VM images. Once again, ***you're back running in 15 minutes or less!*** This method has served me very well and is rock solid time tested!

NOTE: There is a ***caveat!*** If the NAS serving your ***VM image backups*** is virtualized such as (Option-3) Easy Offline Router Migration it will not be able to backup its own VM image! The simple work around for this is to create another NFS netbackups share on a different freeNAS node called netbackups2. Once again, we will use Rsync to automatically synchronize this dataset across all freeNAS nodes. *Please refer to the .3.7-System Diagrams to gain more insight on system architecture and flow.*

KEEP A COPY ON THUMB-DRIVE: Another highly recommended tip is to copy your VM image backups to a thumb-drive or DVD then store them in a fireproof safe. You can easily map a read-only samba share of your VM image backups to be accessible from any windows machine or android phone. Using the small footprint method described in .3-Best Practices ensures your entire VM image backup archive will easily fit on a modern 64-128GB USB thumb-drive.

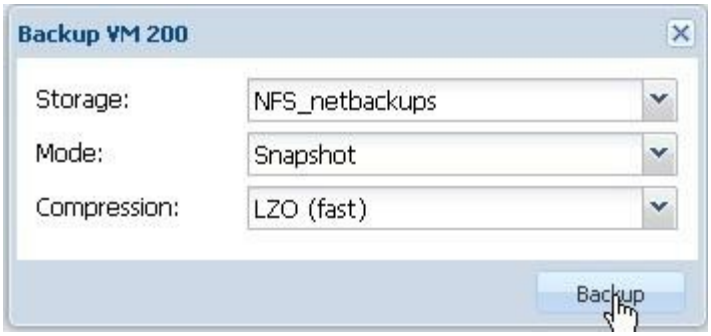
How To Backup Your VM

Proxmox provides you with a convenient backup interface. Simply select the VM you wish to backup from the node tree view and click the Backup tab. Choose your backup location at the far right followed by the **Backup Now** button(pictured below).



You will then be presented with the backup dialog(pictured below).

Choose your options then click **Backup**.



The progress dialog will appear showing the current status of the job(pictured below). That's it!

Task viewer: Backup

Output | Status

Stop

```
INFO: starting new backup job: vzdump 106 --remove 0 --mode snapshot --compress lzo --storage NFS_netbackups --node proxmox2
INFO: Starting Backup of VM 106 (qemu)
INFO: status = running
INFO: update VM 106: -lock backup
INFO: exclude disk 'ide1' (backup=no)
INFO: backup mode: snapshot
INFO: ionice priority: 7
INFO: creating archive '/mnt/pve/NFS_netbackups/dump/vzdump-qemu-106-2015_11_23-11_23_37.vma.lzo'
INFO: started backup task '510d27cd-be8e-43fa-bae3-abd7e9d0346b'
INFO: status: 1% (170131456/8589934592), sparse 0% (30142464), duration 3, 56/46 MB/s
INFO: status: 4% (368705536/8589934592), sparse 0% (66220032), duration 6, 66/54 MB/s
INFO: status: 6% (548470784/8589934592), sparse 0% (66363392), duration 9, 59/59 MB/s
INFO: status: 8% (714932224/8589934592), sparse 0% (66514944), duration 12, 55/55 MB/s
INFO: status: 10% (896204800/8589934592), sparse 1% (94437376), duration 15, 60/51 MB/s
INFO: status: 12% (1093795840/8589934592), sparse 2% (208830464), duration 18, 65/27 MB/s
INFO: status: 15% (1295253504/8589934592), sparse 4% (410288128), duration 21, 67/0 MB/s
INFO: status: 17% (1501429760/8589934592), sparse 7% (616464384), duration 24, 68/0 MB/s
INFO: status: 19% (1701249024/8589934592), sparse 9% (816283648), duration 27, 66/0 MB/s
```

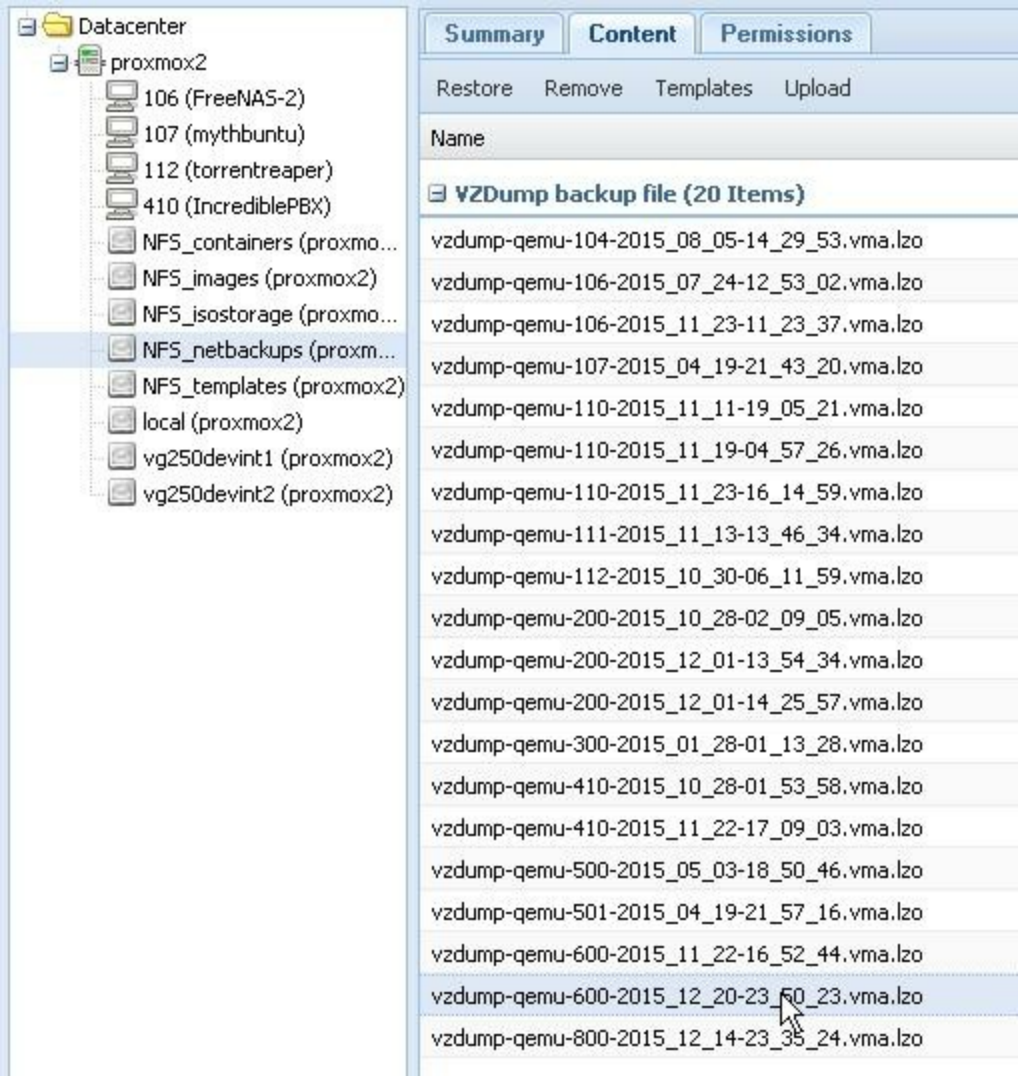
NOTE: Image backups are **NEVER** enough. You will still want to perform traditional backups from within the guest. **IMPORTANT**: I highly recommend that you do **NOT** try to backup VM image disks that are much larger than 80Gb or that use device pass-through(explained in).

For example: The freeNAS VM build covered in Book 3: freeNAS with a 6TB pass-through storage drive should be configured using RSync and configuration backups from within the freeNAS guest.

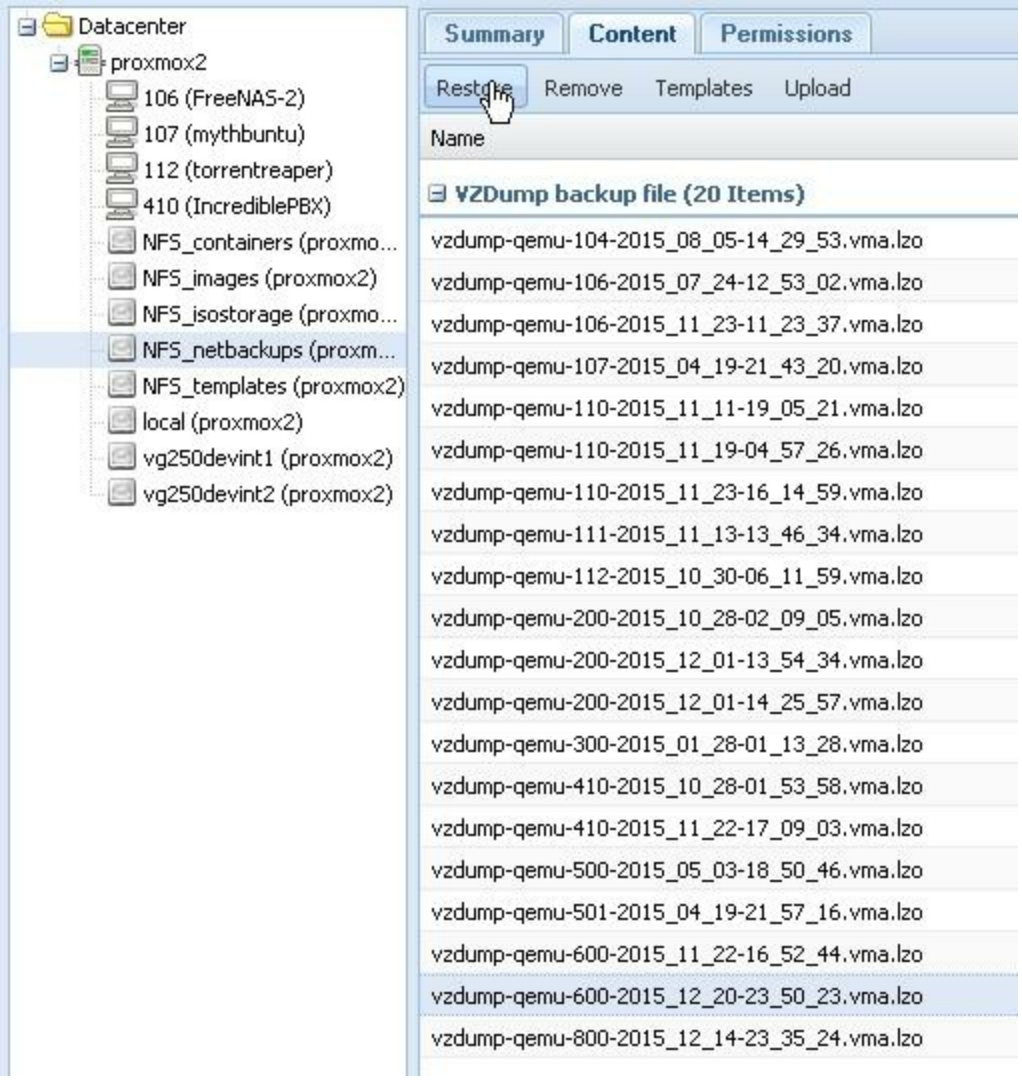
I like to think of Proxmox image backups as a Master Recovery Image. ***Your backup frequency should be very low from within Proxmox(maybe 1 backup every few months).***

How To Restore Your VM

To restore a VM select your backup location in the ***node view tree***. For this example I have selected **NFS_netbackups**(pictured below). Once selected you should see the list of archives under the content tab. Now, choose the archive that you wish to restore(shown below).

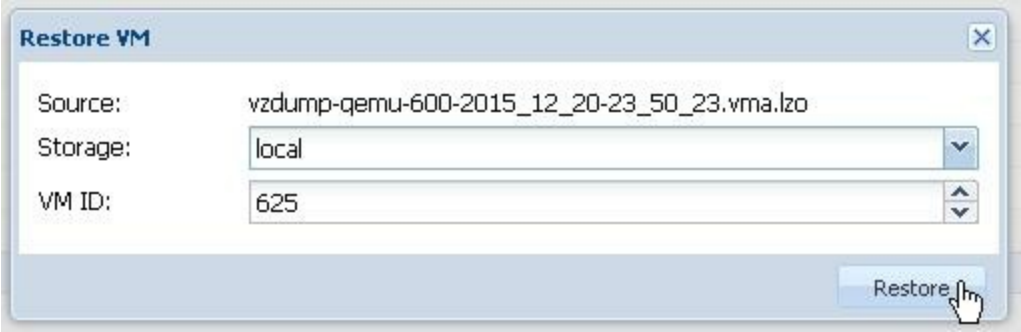


Once you have selected an archive click on **Restore**(pictured below).



You should now see the **Restore VM** dialog(pictured below) where you can assign a new **VM ID** and select the **Storage** location.

When finish click the **Restore** button(shown below).



Once the process begins you will see the ***task viewer*** where you can watch the **status** of your restore(pictured below).

Task viewer: VM 625 - Restore

Output | Status

Stop

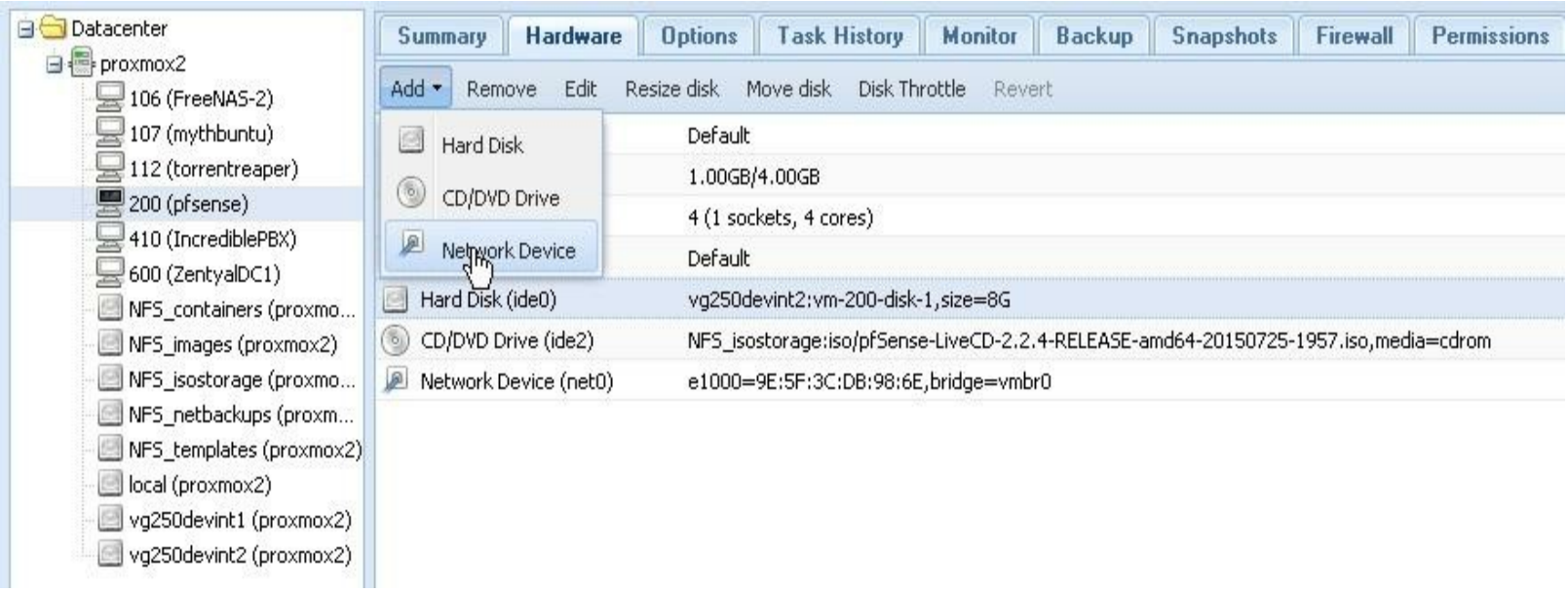
```
restore vma archive: lzop -d -c /mnt/pve/NFS_netbackups/dump/vzdump-qemu-600-2015_12_20-23_50_23.vma.lzo|vma extract -v -r /var/tmp/vzdumptmp4026
CFG: size: 314 name: qemu-server.conf
DEV: dev_id=1 size: 34359738368 devname: drive-ide0
CTIME: Sun Dec 20 23:50:24 2015
Formatting '/var/lib/vz/images/625/vm-625-disk-1.raw', fmt=raw size=34359738368
new volume ID is 'local:625/vm-625-disk-1.raw'
map 'drive-ide0' to '/var/lib/vz/images/625/vm-625-disk-1.raw' (write zeros = 0)
progress 1% (read 343605248 bytes, duration 10 sec)
progress 2% (read 687210496 bytes, duration 18 sec)
progress 3% (read 1030815744 bytes, duration 30 sec)
progress 4% (read 1374420992 bytes, duration 38 sec)
progress 5% (read 1718026240 bytes, duration 46 sec)
progress 6% (read 2061631488 bytes, duration 57 sec)
progress 7% (read 2405236736 bytes, duration 62 sec)
```

1.11-VM Hardware

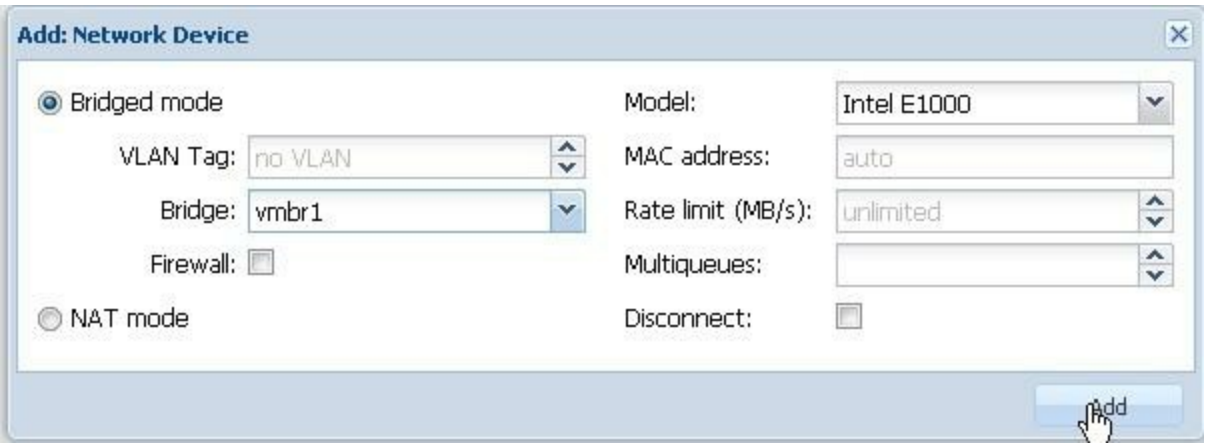
Network Adapters

At some point you may want to add or edit your VM hardware. Proxmox offers a wide range of options including adding, editing, and removing both disk and network adapters. It also allows for moving, throttling, and resizing of disks. You already added a network adapter earlier in this chapter for use with the pfSense router configuration so the hardware tab should not be strange. Once again, for reference to this hardware section we'll add a network adapter as pictured below.

Let's continue: Click **Add** >> **Network Device**

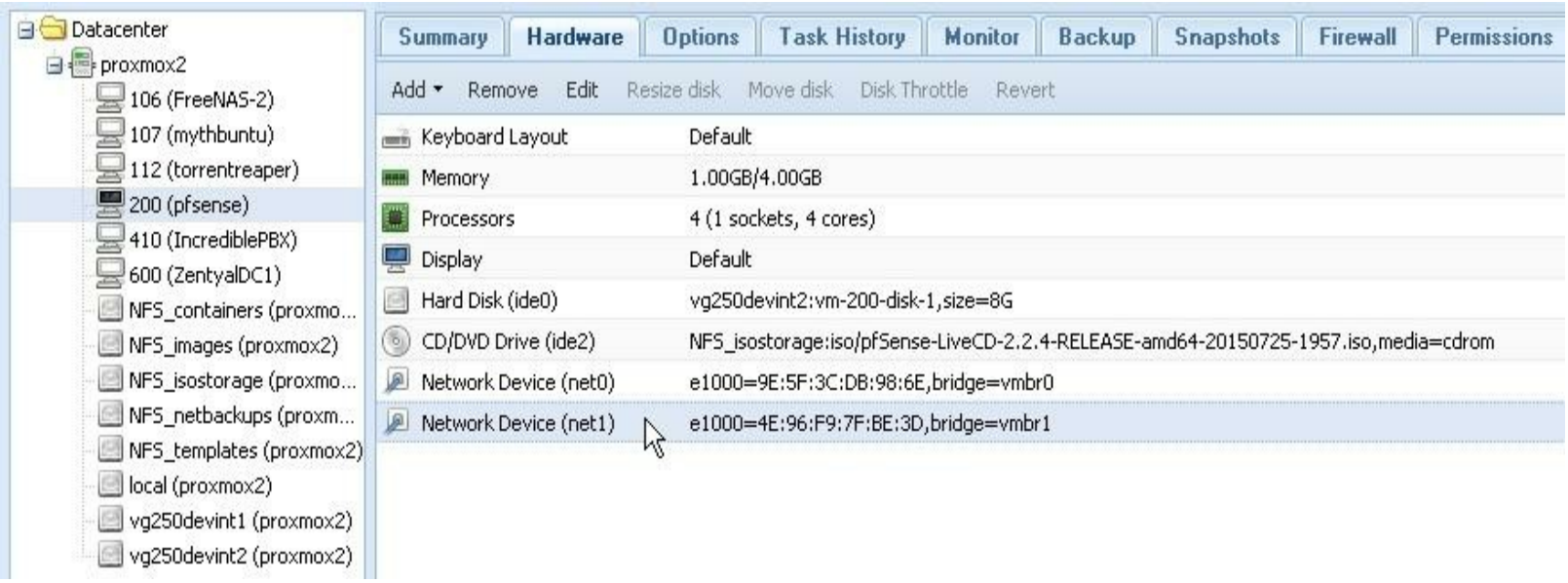


Now add a new network bridge(shown below). For this example I have chosen vmbr1 but that can be changed very easily whenever you want.



Now you will see your newly added adapter in the hardware list(pictured below).

MAC address NOTE: The hardware address you see is an alias and not the actual hardware address!



You can change the Mac address, Model, or Bridge of any selected adapter simply by clicking the edit button under the hardware tab. Figures (1-3) below show the edit network dialog.

fig.1.

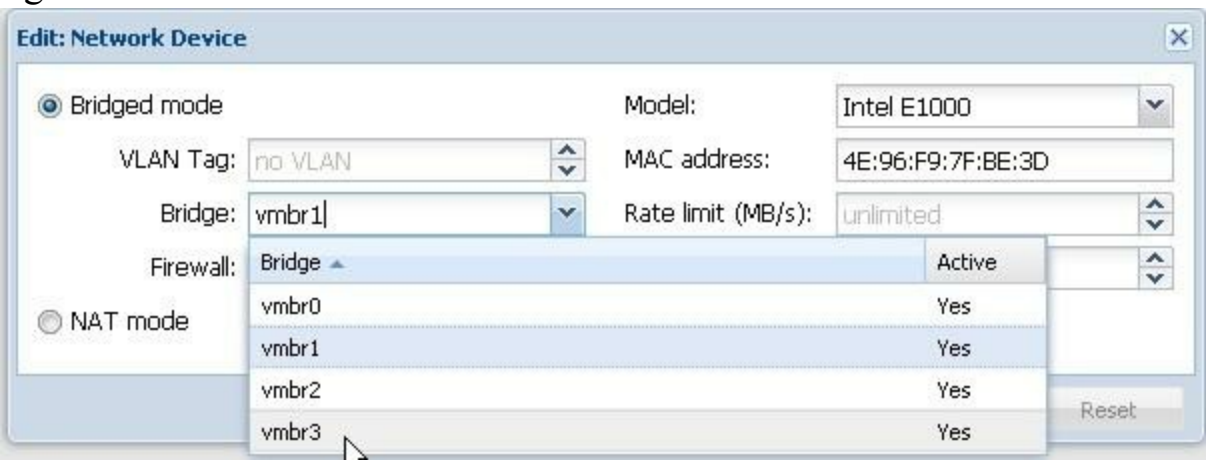


fig.2

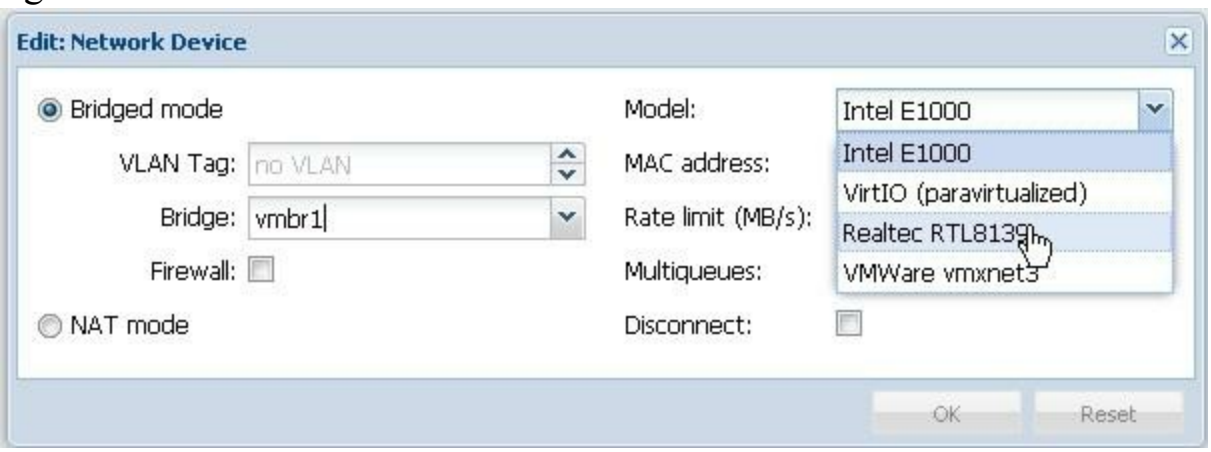
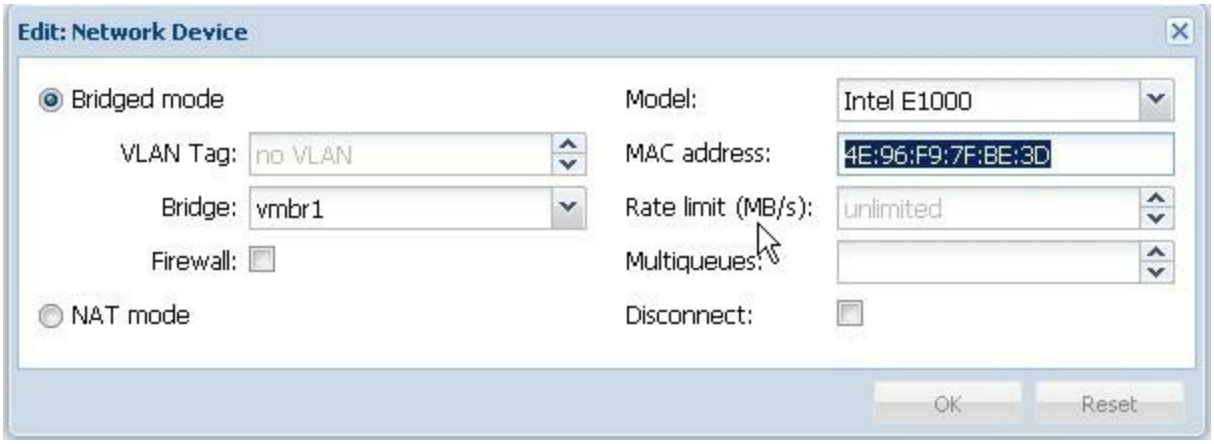
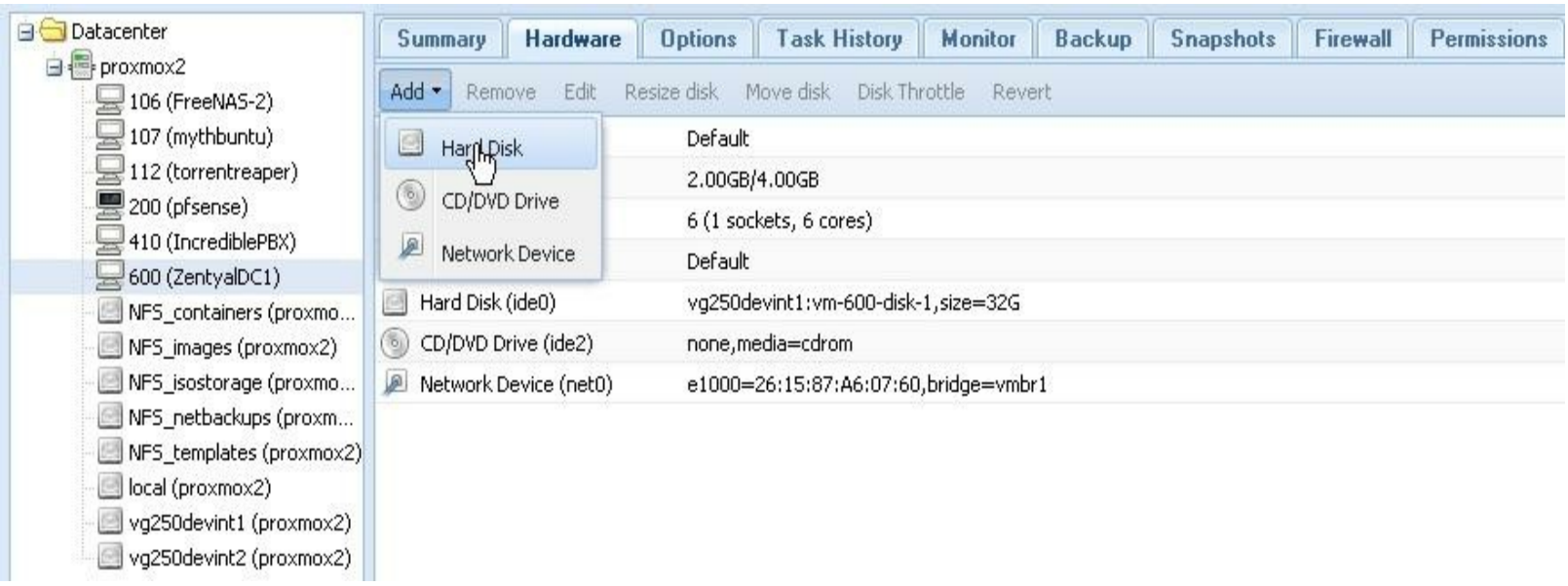


fig.3

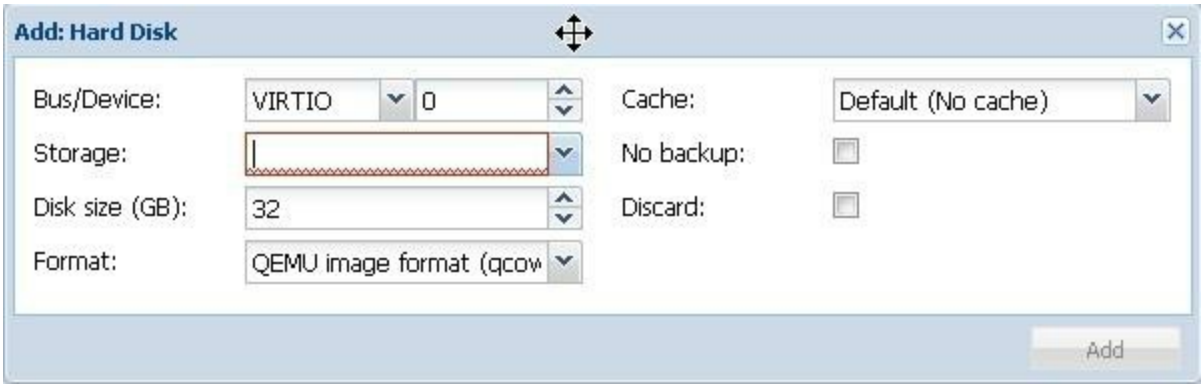


Hard Disk

Adding a new disk is equally simple. Let's create a new 32Gb IDE drive for a Zentyal Domain Controller(shown below). Click **Add** >> **Hard Disk**(pictured below)



You will see the Add: Hard Disk dialog(pictured below). Notice the default Bus is VIRTIO. VIRTIO is a high performance driver but may not be compatible with your installation. For the most compatible least troublesome Bus I recommend IDE. Also notice the default Format is Qcow2. I ALWAYS use Raw format! It is the highest performing and most compatible Format. Also, stick with Cache default to avoid data loss!



Figures (4-6) show the various dropdowns in the Hard Disk dialog. Notice: Incorrectly selected items will appear in red until the proper value is chosen.

fig.4

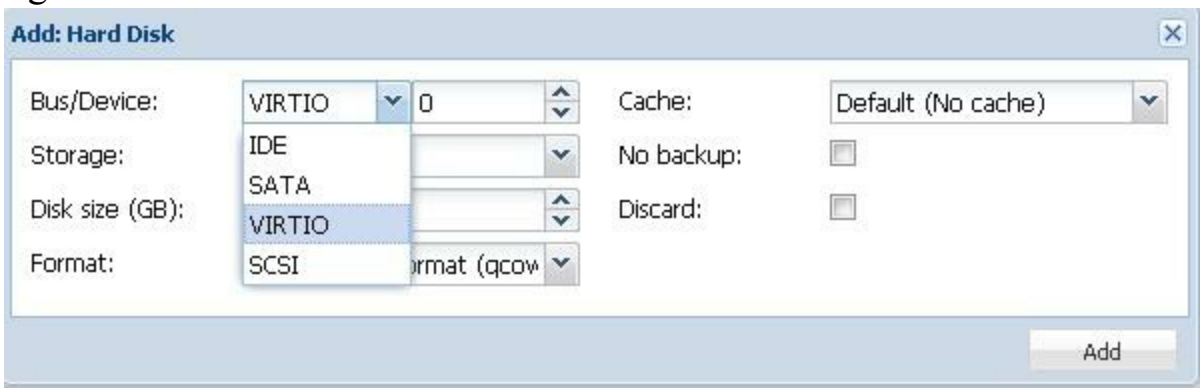


fig.5

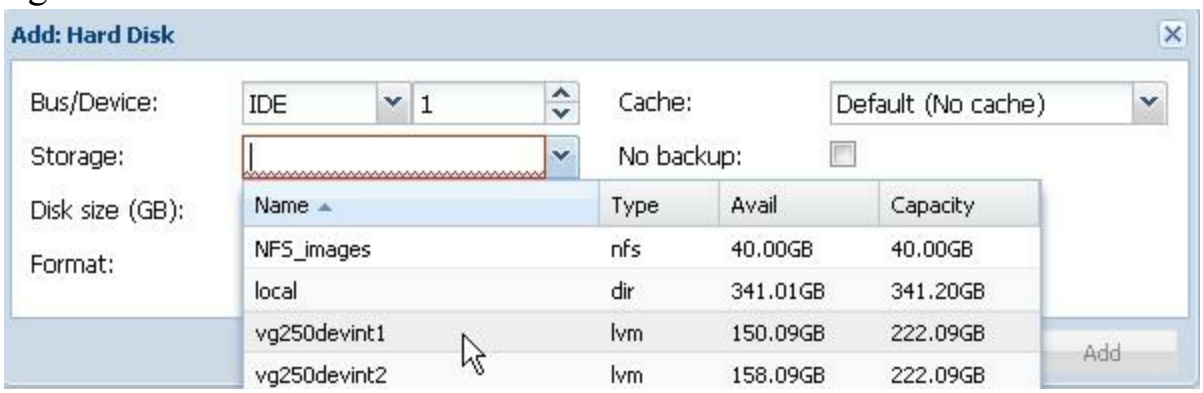
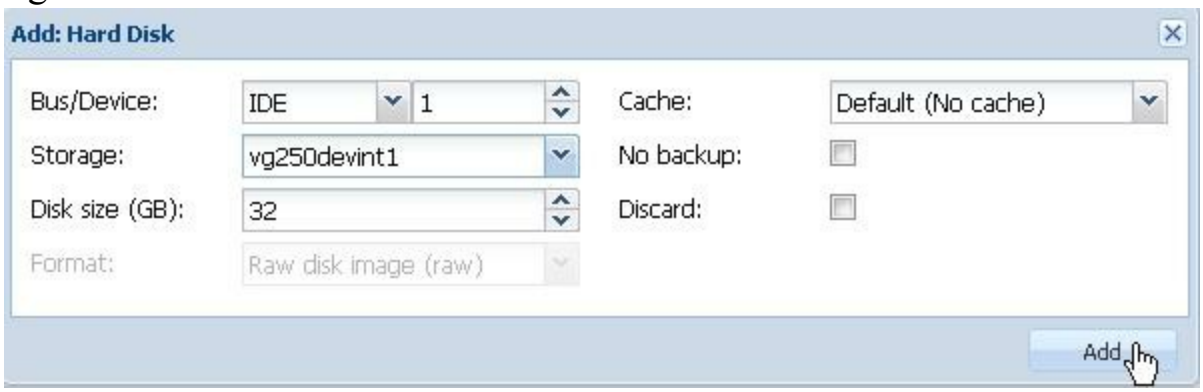
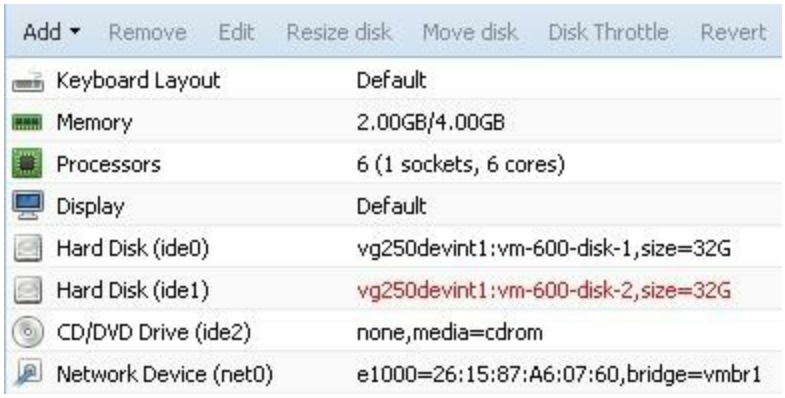


fig.6



Once added your new disk will appear red until the VM is power-cycled(pictured below).



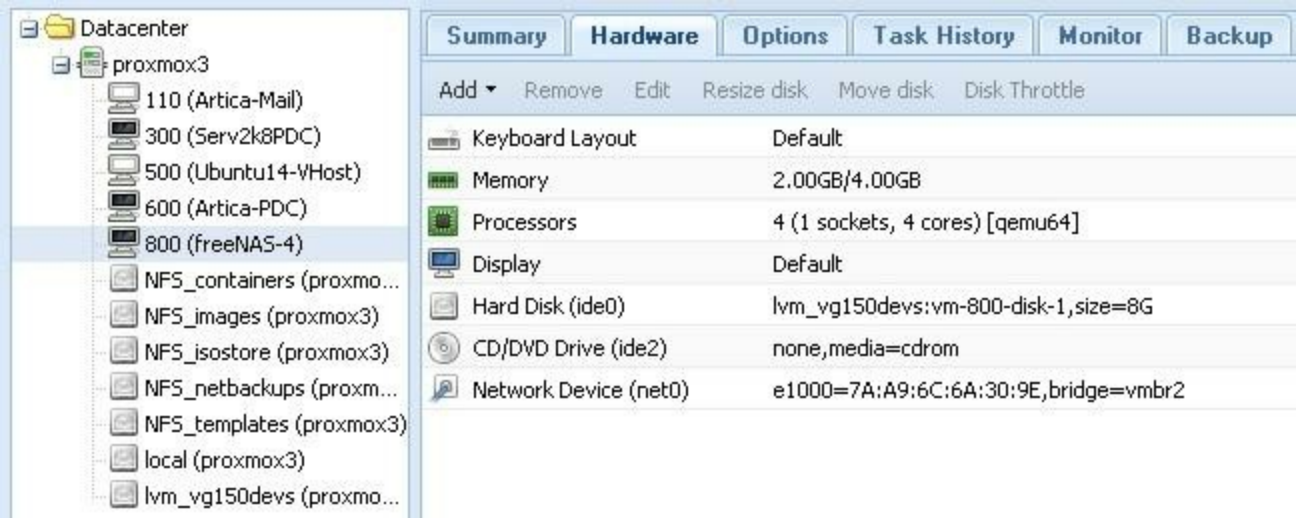
1.12-Adding Pass-Through Disks

As mentioned in the .3-Best Practices section, I use hybrid servers. Essentially, you are creating a Proxmox virtualization host with a ***built in NAS server***. You install the NAS just like any other VM with its OS residing on a virtual disk. However, the actual storage drives will reside on physical LVM storage assigned through a technique known as **hardware pass-through**.

This method allows for a ***very small backup footprint*** because your only backing up the NAS operating system and **NOT** the data. It also provides moderately better disk throughput for data read/write cycles. I have tested sustained throughput rates in the range of 30-60 Megabytes/sec using Gigabit adapters. Bonding your adapters does yield better performance but I like to keep it simple!

The biggest advantage is that your data is **NOT** stored in a virtual disk file! Even if you destroy the VM the data remains safe!

Now that you have an understanding let's add a 6TB striped volume to a new install of freeNAS. As you can see the freeNAS install only has one 8GB IDE disk where the OS resides(pictured below).



Let's open **PuTTY** and login as root on your Proxmox server. Then we need to find our disks using the following command(pictured below):

cat /proc/partitions

```
192.168.0.16 - PuTTY
root@proxmox3:~# cat /proc/partitions
major minor  #blocks  name

   8        0  156290904 sda
   8        1  156289880 sda1
   8       16 2930266584 sdb
   8       17 2147482623 sdb1
   8       32 2930266584 sdc
   8       33 2147482623 sdc1
   8       48  156290904 sdd
   8       49  156289880 sdd1
   8       64   87918264 sde
   8       65       1024 sde1
   8       66     522240 sde2
   8       67   87393280 sde3
 253        0   21757952 dm-0
 253        1   10878976 dm-1
 253        2   43880448 dm-2
 253        3   33554432 dm-3
 253        6   33554432 dm-6
 253        5   33554432 dm-5
 253        8    8388608 dm-8
 253        4   83886080 dm-4
root@proxmox3:~#
```

As you can see, the largest disks(picture above) are /dev/sdb and /dev/sdc.

Also notice that there are /dev/sdb1 and /dev/sdc1 as well. This indicates a ***single partition exists*** on each disk. The partition sizes indicate that all available space is not being used. We need to change that! To edit /dev/sdb type the following command:

fdisk /dev/sdb

You will now see something like this(pictured below):

```
192.168.0.16 - PuTTY
   8       65       1024 sde1
   8       66     522240 sde2
   8       67   87393280 sde3
 253        0   21757952 dm-0
 253        1   10878976 dm-1
 253        2   43880448 dm-2
 253        3   33554432 dm-3
 253        6   33554432 dm-6
 253        5   33554432 dm-5
 253        8    8388608 dm-8
 253        4   83886080 dm-4
root@proxmox3:~# fdisk /dev/sdb

WARNING: The size of this disk is 3.0 TB (3000592982016 bytes).
DOS partition table format can not be used on drives for volumes
larger than (2199023255040 bytes) for 512-byte sectors. Use parted(1) and GUID
partition table format (GPT).


The device presents a logical sector size that is smaller than
the physical sector size. Aligning to a physical sector (or optimal
I/O) size boundary is recommended, or performance may be impacted.

Command (m for help):
```

Now press: **m** >> Enter

You will see the help screen(shown below). We are interested in an creating ***empty DOS partition table***.

```
192.168.0.16 - PuTTY
The device presents a logical sector size that is smaller than
the physical sector size. Aligning to a physical sector (or optimal
I/O) size boundary is recommended, or performance may be impacted.

Command (m for help): m
Command action
   a   toggle a bootable flag
   b   edit bsd disklabel
   c   toggle the dos compatibility flag
   d   delete a partition
   l   list known partition types
   m   print this menu
   n   add a new partition
   o   create a new empty DOS partition table
   p   print the partition table
   q   quit without saving changes
   s   create a new empty Sun disklabel
   t   change a partition's system id
   u   change display/entry units
   v   verify the partition table
   w   write table to disk and exit
   x   extra functionality (experts only)

Command (m for help):
```

Now press: **o** >> Enter

Followed by: **w** >> Enter

This series of commands will create a new ***empty DOS partition table*** and write changes to disk.

Next we need to repeat these steps for /dev/sdc. Do NOT worry about the lack of partitions! The beauty of this method is that **LVM** doesn't care!

Let's verify our disks again to ensure the partitions are gone using the following command:

cat /proc/partitions

```
192.168.0.16 - PuTTY
root@proxmox3:~# cat /proc/partitions
major minor  #blocks  name

   8        0  156290904 sda
   8        1  156289880 sda1
   8       16 2930266584 sdb
   8       32 2930266584 sdc
   8       48  156290904 sdd
   8       49  156289880 sdd1
   8       64   87918264 sde
   8       65       1024 sde1
   8       66     522240 sde2
   8       67   87393280 sde3
 253        0   21757952 dm-0
 253        1   10878976 dm-1
 253        2   43880448 dm-2
 253        3   33554432 dm-3
 253        6   33554432 dm-6
 253        5   33554432 dm-5
 253        4   83886080 dm-4
root@proxmox3:~#
```

As you can see(above), /dev/sdb and /dev/sdc can now be used to ***full capacity***.

We will now create LVM ***physical volumes***(PV's) using the following commands:

pvcreate /dev/sdb

pvcreate /dev/sdc

OR

pvcreate /dev/sd[b,c]

```
192.168.0.16 - PuTTY
major minor  #blocks  name

   8        0  156290904 sda
   8        1  156289880 sda1
   8       16 2930266584 sdb
   8       32 2930266584 sdc
   8       48  156290904 sdd
   8       49  156289880 sdd1
   8       64   87918264 sde
   8       65       1024 sde1
   8       66     522240 sde2
   8       67   87393280 sde3
 253        0   21757952 dm-0
 253        1   10878976 dm-1
 253        2   43880448 dm-2
 253        3   33554432 dm-3
 253        6   33554432 dm-6
 253        5   33554432 dm-5
 253        8    8388608 dm-8
 253        4   83886080 dm-4
root@proxmox3:~# pvcreate /dev/sd[b,c]
  Physical volume "/dev/sdb" successfully created
  Physical volume "/dev/sdc" successfully created
root@proxmox3:~#
```

The output above shows successful creation.

Next, we will create a ***volume group***(VG) containing both disks with the following command:

vgcreate freenas4 /dev/sd[b,c]

```
192.168.0.16 - PuTTY
   8        0  156290904 sda
   8        1  156289880 sda1
   8       16 2930266584 sdb
   8       32 2930266584 sdc
   8       48  156290904 sdd
   8       49  156289880 sdd1
   8       64   87918264 sde
   8       65       1024 sde1
   8       66     522240 sde2
   8       67   87393280 sde3
 253        0   21757952 dm-0
 253        1   10878976 dm-1
 253        2   43880448 dm-2
 253        3   33554432 dm-3
 253        6   33554432 dm-6
 253        5   33554432 dm-5
 253        8    8388608 dm-8
 253        4   83886080 dm-4
root@proxmox3:~# pvcreate /dev/sd[b,c]
  Physical volume "/dev/sdb" successfully created
  Physical volume "/dev/sdc" successfully created
root@proxmox3:~# vgcreate freenas4 /dev/sd[b,c]
  Volume group "freenas4" successfully created
root@proxmox3:~#
```

The output above shows our VG created successfully.

For the final step we will create a striped ***logical volume***(LV) using all available space. **LVM Striping** is equivalent to **RAID-0** for ***maximum*** disk throughput.

Type the following command to create the stripe:

lvcreate -l 100%FREE -i2 -n 6tbstore freenas4

where: i2(number of stripe members), n(name)

```
192.168.0.16 - PuTTY
   8       32 2930266584 sdc
   8       48  156290904 sdd
   8       49  156289880 sdd1
   8       64   87918264 sde
   8       65       1024 sde1
   8       66     522240 sde2
   8       67   87393280 sde3
 253        0   21757952 dm-0
 253        1   10878976 dm-1
 253        2   43880448 dm-2
 253        3   33554432 dm-3
 253        6   33554432 dm-6
 253        5   33554432 dm-5
 253        8    8388608 dm-8
 253        4   83886080 dm-4
root@proxmox3:~# pvcreate /dev/sd[b,c]
  Physical volume "/dev/sdb" successfully created
  Physical volume "/dev/sdc" successfully created
root@proxmox3:~# vgcreate freenas4 /dev/sd[b,c]
  Volume group "freenas4" successfully created
root@proxmox3:~# lvcreate -l 100%FREE -i2 -n 6tbstore freenas4
  Using default stripesize 64.00 KiB
  Logical volume "6tbstore" created
root@proxmox3:~#
```

The above output shows our LV stripe successfully created.

As I mentioned earlier, Linux **LVM** is ***extremely*** powerful and flexible. I would highly recommend learning it well. Below are 3 more very useful LVM commands:

pvscan

This command lists **ALL** known physical volumes(pictured below).

```
192.168.0.16 - PuTTY
 253        0   21757952 dm-0
 253        1   10878976 dm-1
 253        2   43880448 dm-2
 253        3   33554432 dm-3
 253        6   33554432 dm-6
 253        5   33554432 dm-5
 253        8    8388608 dm-8
 253        4   83886080 dm-4
root@proxmox3:~# pvcreate /dev/sd[b,c]
  Physical volume "/dev/sdb" successfully created
  Physical volume "/dev/sdc" successfully created
root@proxmox3:~# vgcreate freenas4 /dev/sd[b,c]
  Volume group "freenas4" successfully created
root@proxmox3:~# lvcreate -l 100%FREE -i2 -n 6tbstore freenas4
  Using default stripesize 64.00 KiB
  Logical volume "6tbstore" created
root@proxmox3:~# pvscan
  PV /dev/sde3   VG pve         lvm2 [83.34 GiB / 10.37 GiB free]
  PV /dev/sdb    VG freenas4    lvm2 [2.73 TiB / 0    free]
  PV /dev/sdc    VG freenas4    lvm2 [2.73 TiB / 0    free]
  PV /dev/sda1   VG vg150devs   lvm2 [149.05 GiB / 45.05 GiB free]
  PV /dev/sdd1   VG vg150devs   lvm2 [149.05 GiB / 69.05 GiB free]
  Total: 5 [5.83 TiB] / in use: 5 [5.83 TiB] / in no VG: 0 [0   ]
root@proxmox3:~#
```

vgscan

This command lists **ALL** known volume groups(pictured below).

```
192.168.0.16 - PuTTY
 253        5   33554432 dm-5
 253        8    8388608 dm-8
 253        4   83886080 dm-4
root@proxmox3:~# pvcreate /dev/sd[b,c]
  Physical volume "/dev/sdb" successfully created
  Physical volume "/dev/sdc" successfully created
root@proxmox3:~# vgcreate freenas4 /dev/sd[b,c]
  Volume group "freenas4" successfully created
root@proxmox3:~# lvcreate -l 100%FREE -i2 -n 6tbstore freenas4
  Using default stripesize 64.00 KiB
  Logical volume "6tbstore" created
root@proxmox3:~# pvscan
  PV /dev/sde3   VG pve         lvm2 [83.34 GiB / 10.37 GiB free]
  PV /dev/sdb    VG freenas4    lvm2 [2.73 TiB / 0    free]
  PV /dev/sdc    VG freenas4    lvm2 [2.73 TiB / 0    free]
  PV /dev/sda1   VG vg150devs   lvm2 [149.05 GiB / 45.05 GiB free]
  PV /dev/sdd1   VG vg150devs   lvm2 [149.05 GiB / 69.05 GiB free]
  Total: 5 [5.83 TiB] / in use: 5 [5.83 TiB] / in no VG: 0 [0   ]
root@proxmox3:~# vgscan
  Reading all physical volumes.  This may take a while...
  Found volume group "pve" using metadata type lvm2
  Found volume group "freenas4" using metadata type lvm2
  Found volume group "vg150devs" using metadata type lvm2
root@proxmox3:~#
```

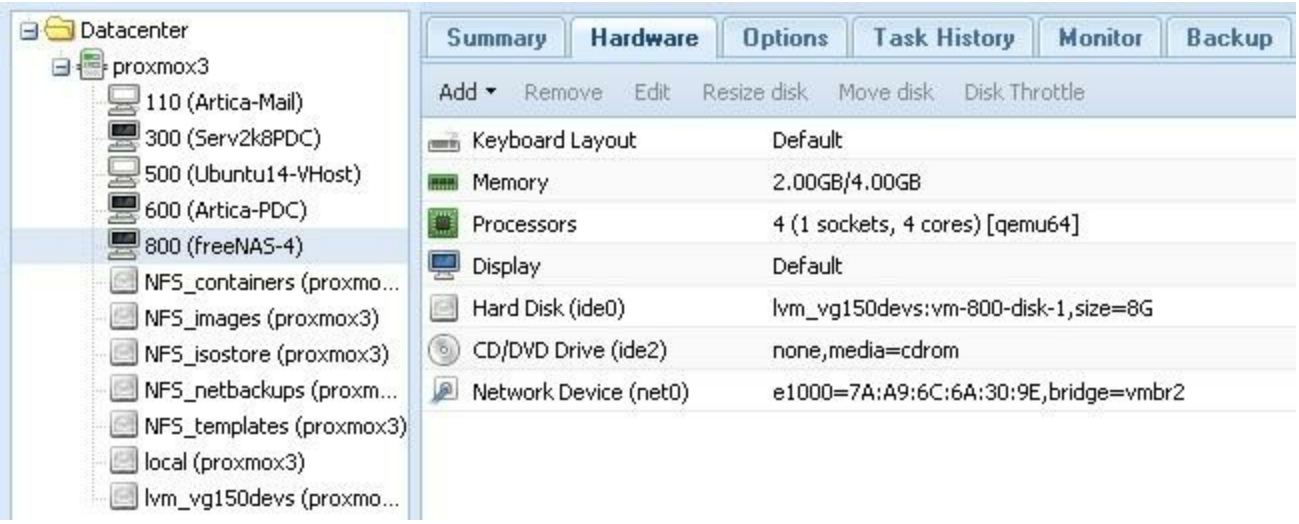
lvscan

This command lists **ALL** known logical volumes(pictured below).

```
192.168.0.16 - PuTTY
  Logical volume "6tbstore" created
root@proxmox3:~# pvscan
  PV /dev/sde3   VG pve         lvm2 [83.34 GiB / 10.37 GiB free]
  PV /dev/sdb    VG freenas4    lvm2 [2.73 TiB / 0    free]
  PV /dev/sdc    VG freenas4    lvm2 [2.73 TiB / 0    free]
  PV /dev/sda1   VG vg150devs   lvm2 [149.05 GiB / 45.05 GiB free]
  PV /dev/sdd1   VG vg150devs   lvm2 [149.05 GiB / 69.05 GiB free]
  Total: 5 [5.83 TiB] / in use: 5 [5.83 TiB] / in no VG: 0 [0   ]
root@proxmox3:~# vgscan
  Reading all physical volumes.  This may take a while...
  Found volume group "pve" using metadata type lvm2
  Found volume group "freenas4" using metadata type lvm2
  Found volume group "vg150devs" using metadata type lvm2
root@proxmox3:~# lvscan
  ACTIVE            '/dev/pve/swap' [10.38 GiB] inherit
  ACTIVE            '/dev/pve/root' [20.75 GiB] inherit
  ACTIVE            '/dev/pve/data' [41.85 GiB] inherit
  ACTIVE            '/dev/freenas4/6tbstore' [5.46 TiB] inherit
  ACTIVE            '/dev/vg150devs/vm-300-disk-1' [32.00 GiB] inherit
  ACTIVE            '/dev/vg150devs/vm-500-disk-1' [80.00 GiB] inherit
  ACTIVE            '/dev/vg150devs/vm-600-disk-1' [32.00 GiB] inherit
  ACTIVE            '/dev/vg150devs/vm-110-disk-1' [32.00 GiB] inherit
  ACTIVE            '/dev/vg150devs/vm-800-disk-1' [8.00 GiB] inherit
root@proxmox3:~#
```

You can see the newly created 6TB striped volume above. Now we're ready to assign this volume to

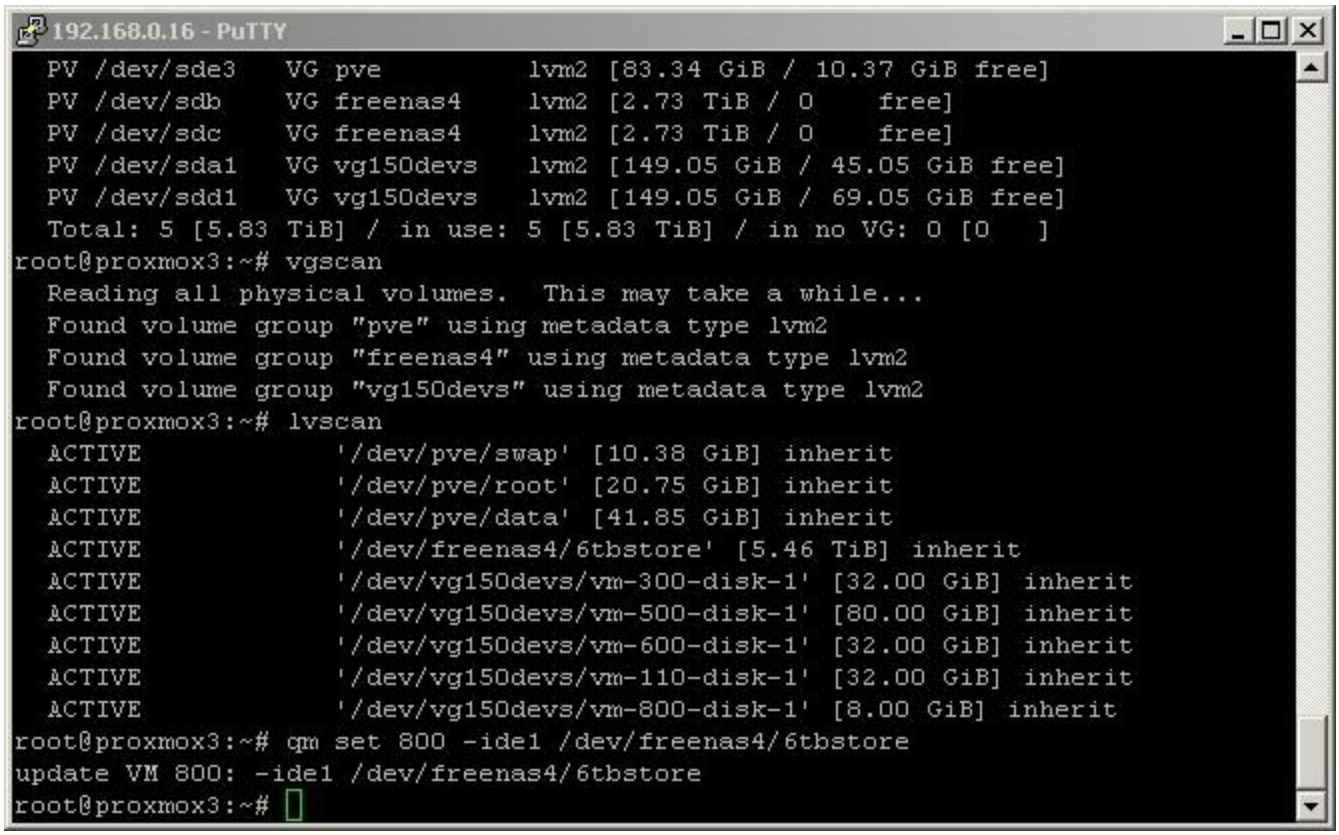
the freeNAS-4 VM. You will notice the ID number of freeNAS-4 is 800 and IDE1 or IDE3 is available(pictured below).



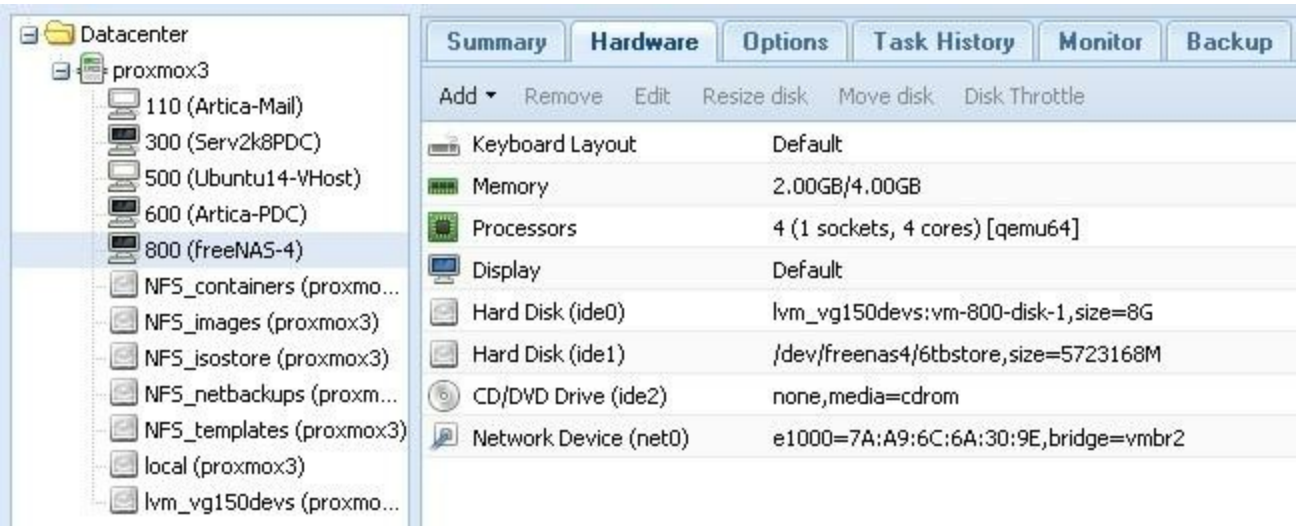
To assign the new disk we will issue the special **QEMU** command as follows:

qm set 800 -ide1 /dev/freenas4/6tbstore

The command entered into PuTTY looks like this(pictured below).



The result of this command is evident by the new IDE1 drive shown in the freeNAS-4 hardware window(pictured below). **NOTE**: You will need to refresh the tab page before the new disk will appear.



The freeNAS-4 VM(above) could now be booted and the new 6TB disk configured as a ZFS stripe.

PLEASE REMEMBER: It is important to note that freeNAS-4 is now tied to the Proxmox3 server by its hardware pass-through disk. It cannot be moved to another physical machine unless the physical disks are removed. The other VM's(pictured above) can be moved to another physical machine easily using a simple backup/restore. They are NOT tied in any way to the Proxmox3 server.

1.13-Troubleshooting Proxmox

Troubleshooting Proxmox is easy! There isn't any! You may occasionally have a VM locked. Simply issue the following command:

qm unlock [vm-ID]

Example: # qm unlock 800

where 800 is the vm- ID number(pictured above) in node tree view

You may also have a new VM configuration fail to boot. Changing the CPU type from KVM to QEMU or from QEMU to KVM usually works.

Finally: Some operating systems may require you to partition and format the VM disk before they will boot.

1.14-Upgrading Proxmox

When it comes to updates and upgrades to Proxmox I have found the **KISS**(keep it simple stupid) method works the best. **DO NOT** under **ANY** circumstance try to update or upgrade a perfectly functional install! Linux is not like Windows! When things go wrong they tend to go wrong in a **VERY** bad way!

There are ways of updating using apt and aptitude commands but I DO NOT recommend this and it would take a whole chapter just to cover. ***You will spend less time if you simply backup your VM's, restore them to different nodes, then re-install the Proxmox node in question with the latest distribution release.***

With the DVD it takes 10-15 minutes to install and configure! Through command line upgrade it can take 45-60 minutes ***IF*** everything goes right! That's a ***BIG IF***! When you're the only IT Administrator with 200 machines/users to babysit you tend to avoid the ***IF*** scenarios and go with the **sure shot every time**!

Book 2: pfSense

2.1-Introduction To pfSense

About 1 year after placing Proxmox in production at work I got a call. I was told that one client decided to change encryption on our VPN tunnel to something more secure. I soon realized that our existing equipment could NOT be upgraded so I began searching for alternatives. That's when I decided on pfSense!

My first install was bare metal and worked just fine. It wasn't long before I began pondering the idea of a virtualized routing platform. The great debate was whether virtualized routers were up to the task from a security standpoint. I just couldn't let the idea rest unless I tried it! Well, I must say, that 7 years later I'm glad I decided to virtualize.

The security question was soon put to the test after experiencing some issues with an ATT gateway. I ended up spending the whole day on the phone with ATT starting at level-1 and eventually making it to TOP level-6 support. This is where the network engineers spend their days! To make a long story short, **ATT Network Engineers could NOT test my gateways without pfSense being disabled**.

Over the years **Snort IDS** running on pfSense has caught numerous offenders and **killed the connections immediately**. Whenever I install new software it's packet sniffed with **Wireshark** before ever going into production! Furthermore, network monitors such as **Nagios Core** provide a wealth of information to keep IT Administrators informed. With ***proper firewall rules*** and ***Layer-2 hardware filtering*** it is **EXTREMELY** unlikely that you will be hacked!

NOTE: pfSense is a powerful platform and it's feature-set cannot be completely covered in this book. This guide was designed as a step-by-step to get you up and running quickly. I highly recommend tapping the wealth of online resources available for a more thorough understanding.

Ok! Enough said! Before installation can begin you must ***create the VM configuration***. I recommend a ***8Gb IDE virtual disk*** with ***4Gb of Ram*** for this install. If you need to review those steps again click here: 1.9-Creating VM Configuration

2.2-Installing pfSense

Now, power on the pfSense VM making sure that you have the CD or disk image loaded.

You should see the following screens:

```
Welcome to pfSense

1. Boot Multi User [Enter]
2. Boot [S]ingle User
3. [Esc]ape to loader prompt
4. Reboot

Options:
5. [K]ernel: kernel (1 of 2)
6. Configure Boot [O]ptions...

Autoboot in 3 seconds. [Space] to pause
```

Now, when you see the prompt(shown below) **press the (I) key**. If you don't catch it in time just reset the VM.

```
Welcome to pfSense 2.2.4-RELEASE  ...

Mounting unionfs directories...done.
Creating symlinks......ELF ldconfig path: /lib /usr/lib /usr/lib/compat /usr/loc
al/lib
32-bit compatibility ldconfig path: /usr/lib32
done.
Launching the init system... done.
Initializing..................... done.
Starting device manager (devd)...done.

[ Press R to enter recovery mode or ]
[  press I to launch the installer  ]

(R)ecovery mode can assist by rescuing config.xml
from a broken hard disk installation, etc.

(I)nstaller may be invoked now if you do
not wish to boot into the liveCD environment at this time.

(C) continues the LiveCD bootup without further pause.

Timeout before auto boot continues (seconds): 6
```

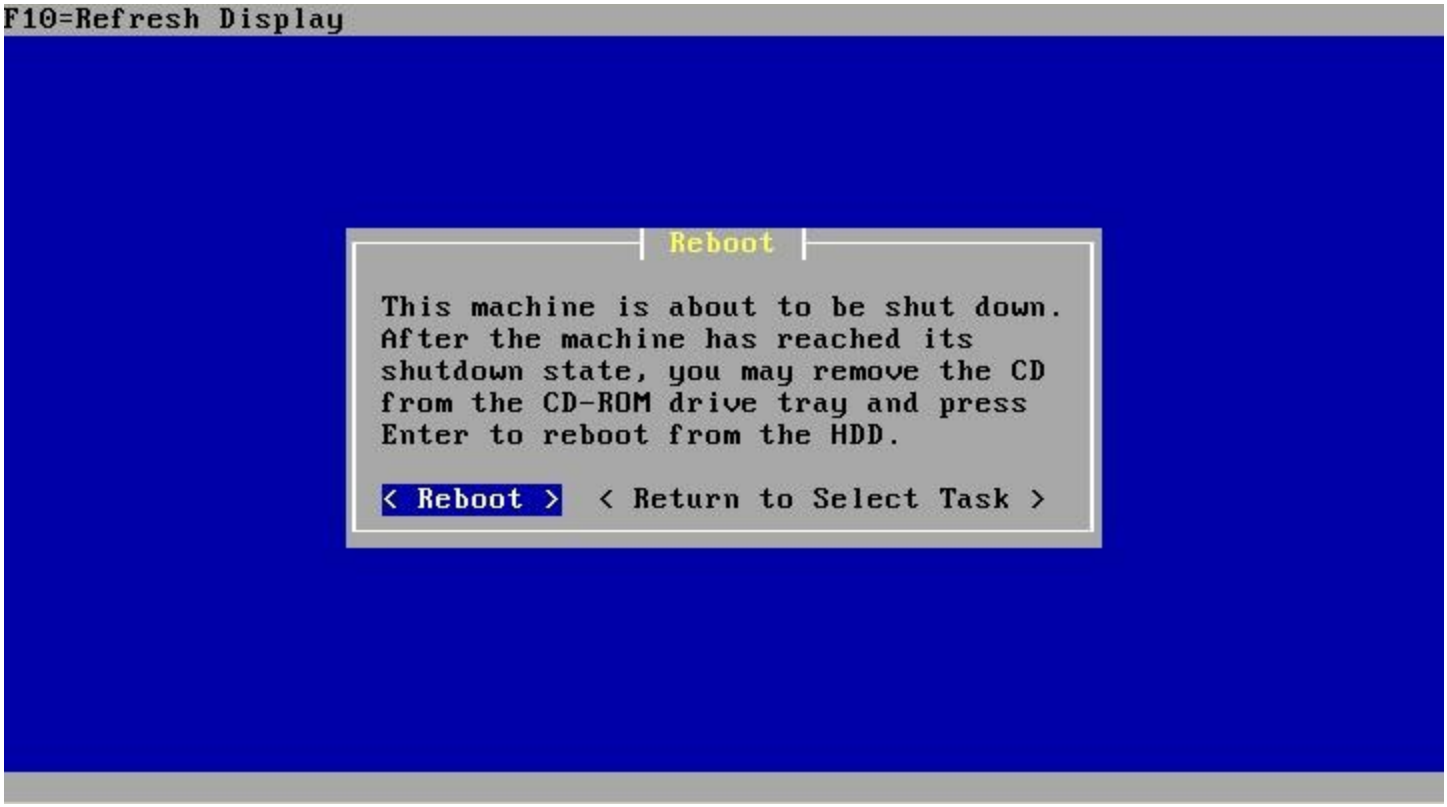
Next you will see the configuration console(pictured below). Use your arrow down to **Accept These Settings** followed by the **Enter** key.

Now, choose the **Quick/Easy Install** (pictured below)

Hit **OK** (pictured below)

You will want to select the **Standard Kernel** (pictured below) for our install.

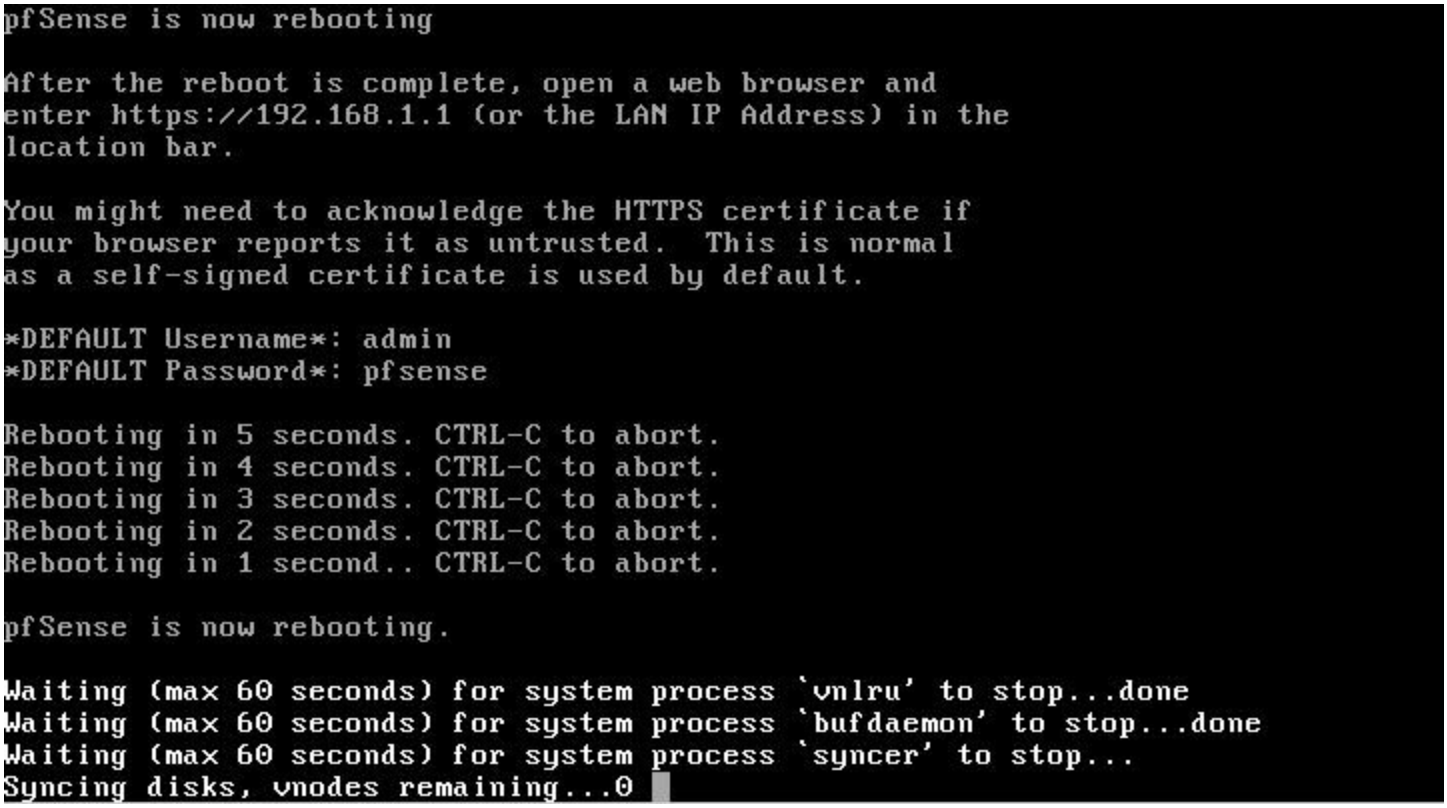
Next, select **Reboot** (pictured below).



When the system reboots you will notice the **DEFAULT** credentials are:

Username: **admin**

Password: **pfsense**



2.3-Assigning Network Interfaces

Next, you will setup the network! Since pfSense is a **BSD** based distribution your network interfaces are ***named differently***. If you have used **e1000 Gigabit** they will show up as **em**(x). If you have used **Realtek** adapters they will be named **re**(x). ***Please pay close attention now***! This is the only tricky part to the install!

Notice in the picture below that **em1** has been **assigned** an **IP Address** and is defaulted to the **LAN** interface. This is NOT correct! The **ONLY** possible way a **DHCP** address could have been assigned is if the ***em1 interface (pictured below) was actually connected to the Internet Router***. We need to flip these interfaces around so the **LAN** becomes **em0**.

NOTE: I find it easiest to **ALWAYS** set the **LAN** to the first interface which is **ALWAYS** going to be **em0** or **re0**.

To assign **em0** to the **LAN** select option **1** then press **ENTER**

```
Configuring firewall......done.
Generating RRD graphs...done.
Starting syslog...done.
Starting CRON... done.
pfSense (pfSense) 2.2.4-RELEASE amd64 Sat Jul 25 19:57:37 CDT 2015
Bootup complete

FreeBSD/amd64 (pfSense.localdomain) (ttyv0)

*** Welcome to pfSense 2.2.4-RELEASE-pfSense (amd64) on pfSense ***

 WAN (wan)       -> em0        ->
 LAN (lan)       -> em1        -> v4: 192.168.1.1/24
 0) Logout (SSH only)                  9) pfTop
 1) Assign Interfaces                 10) Filter Logs
 2) Set interface(s) IP address       11) Restart webConfigurator
 3) Reset webConfigurator password    12) pfSense Developer Shell
 4) Reset to factory defaults         13) Upgrade from console
 5) Reboot system                     14) Enable Secure Shell (sshd)
 6) Halt system                       15) Restore recent configuration
 7) Ping host                         16) Restart PHP-FPM
 8) Shell


Enter an option:
```

You will see the following prompt(pictured below). Type **n** for **NO** then press **ENTER**. We do **NOT** want **VLAN**. Also notice the interface mac addresses. These should match those in your Proxmox vm configuration.

```
 2) Set interface(s) IP address       11) Restart webConfigurator
 3) Reset webConfigurator password    12) pfSense Developer Shell
 4) Reset to factory defaults         13) Upgrade from console
 5) Reboot system                     14) Enable Secure Shell (sshd)
 6) Halt system                       15) Restore recent configuration
 7) Ping host                         16) Restart PHP-FPM
 8) Shell


Enter an option: 1


Valid interfaces are:

em0    4e:d9:aa:95:8f:ad   (up) Intel(R) PRO/1000 Legacy Network Connection 1.0.
6
em1    82:db:d2:02:6d:e2   (up) Intel(R) PRO/1000 Legacy Network Connection 1.0.
6

Do you want to set up VLANs first?

If you are not going to use VLANs, or only for optional interfaces, you should
say no here and use the webConfigurator to configure VLANs later, if required.

Do you want to set up VLANs now [y|n]?
```

Next, you will be prompted for the WAN interface name. Type **em1** then press **ENTER**.

```
 8) Shell


Enter an option: 1


Valid interfaces are:

em0    4e:d9:aa:95:8f:ad   (up) Intel(R) PRO/1000 Legacy Network Connection 1.0.
6
em1    82:db:d2:02:6d:e2   (up) Intel(R) PRO/1000 Legacy Network Connection 1.0.
6

Do you want to set up VLANs first?

If you are not going to use VLANs, or only for optional interfaces, you should
say no here and use the webConfigurator to configure VLANs later, if required.

Do you want to set up VLANs now [y|n]? n

If you do not know the names of your interfaces, you may choose to use
auto-detection. In that case, disconnect all interfaces now before
hitting 'a' to initiate auto detection.

Enter the WAN interface name or 'a' for auto-detection: em1
```

pfSense will now ask for the **LAN** interface name(pictured below). Type **em0** then press **ENTER**.

```
Valid interfaces are:

em0    4e:d9:aa:95:8f:ad   (up) Intel(R) PRO/1000 Legacy Network Connection 1.0.
6
em1    82:db:d2:02:6d:e2   (up) Intel(R) PRO/1000 Legacy Network Connection 1.0.
6

Do you want to set up VLANs first?

If you are not going to use VLANs, or only for optional interfaces, you should
say no here and use the webConfigurator to configure VLANs later, if required.

Do you want to set up VLANs now [y|n]? n

If you do not know the names of your interfaces, you may choose to use
auto-detection. In that case, disconnect all interfaces now before
hitting 'a' to initiate auto detection.

Enter the WAN interface name or 'a' for auto-detection: em1

Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(or nothing if finished): em0
```

Since we will **NOT** setup an optional interface(**opt1**) right now simply press the **ENTER** key which indicates NO SELECTION(pictured below).

```
em0    4e:d9:aa:95:8f:ad   (up) Intel(R) PRO/1000 Legacy Network Connection 1.0.
6
em1    82:db:d2:02:6d:e2   (up) Intel(R) PRO/1000 Legacy Network Connection 1.0.
6

Do you want to set up VLANs first?

If you are not going to use VLANs, or only for optional interfaces, you should
say no here and use the webConfigurator to configure VLANs later, if required.

Do you want to set up VLANs now [y|n]? n

If you do not know the names of your interfaces, you may choose to use
auto-detection. In that case, disconnect all interfaces now before
hitting 'a' to initiate auto detection.

Enter the WAN interface name or 'a' for auto-detection: em1

Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(or nothing if finished): em0

Enter the Optional 1 interface name or 'a' for auto-detection
(or nothing if finished):
```

Your interfaces will now be assigned(shown below). Type **y** then press **ENTER**.

```
If you are not going to use VLANs, or only for optional interfaces, you should
say no here and use the webConfigurator to configure VLANs later, if required.

Do you want to set up VLANs now [y|n]? n

If you do not know the names of your interfaces, you may choose to use
auto-detection. In that case, disconnect all interfaces now before
hitting 'a' to initiate auto detection.

Enter the WAN interface name or 'a' for auto-detection: em1

Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(or nothing if finished): em0

Enter the Optional 1 interface name or 'a' for auto-detection
(or nothing if finished):

The interfaces will be assigned as follows:

WAN  -> em1
LAN  -> em0

Do you want to proceed [y|n]?y
```

2.3-Assigning IP Addresses

Now you will need to set the IP address of the **LAN** adapter This will be the address the web interface runs on. It will also serve as the ***default gateway*** and ***DNS server*** on your local network. NOTE: I prefer to set this address as the last in the subnet(**x.x.x.254**).

To proceed: select option **2** then press **ENTER**

```
The interfaces will be assigned as follows:

WAN  -> em1
LAN  -> em0

Do you want to proceed [y|n]?y

Writing configuration...done.
One moment while we reload the settings... done!
*** Welcome to pfSense 2.2.4-RELEASE-pfSense (amd64) on pfSense ***

 WAN (wan)       -> em1        -> v4/DHCP4: 192.168.1.105/24
 LAN (lan)       -> em0        ->
 0) Logout (SSH only)                  9) pfTop
 1) Assign Interfaces                 10) Filter Logs
 2) Set interface(s) IP address       11) Restart webConfigurator
 3) Reset webConfigurator password    12) pfSense Developer Shell
 4) Reset to factory defaults         13) Upgrade from console
 5) Reboot system                     14) Enable Secure Shell (sshd)
 6) Halt system                       15) Restore recent configuration
 7) Ping host                         16) Restart PHP-FPM
 8) Shell


Enter an option:
```

Next, type the number of the interface you wish to configure. In our case we want the LAN adapter which is number 2 in the list(pictured below).

To proceed: Type **2** then press **ENTER**

```
Writing configuration...done.
One moment while we reload the settings... done!
*** Welcome to pfSense 2.2.4-RELEASE-pfSense (amd64) on pfSense ***

 WAN (wan)       -> em1        -> v4/DHCP4: 192.168.1.105/24
 LAN (lan)       -> em0        ->
 0) Logout (SSH only)                   9) pfTop
 1) Assign Interfaces                  10) Filter Logs
 2) Set interface(s) IP address        11) Restart webConfigurator
 3) Reset webConfigurator password     12) pfSense Developer Shell
 4) Reset to factory defaults          13) Upgrade from console
 5) Reboot system                      14) Enable Secure Shell (sshd)
 6) Halt system                        15) Restore recent configuration
 7) Ping host                          16) Restart PHP-FPM
 8) Shell


Enter an option: 2

Available interfaces:

1 - WAN (em1 - dhcp, dhcp6)
2 - LAN (em0 - static)

Enter the number of the interface you wish to configure:
```

You will now be prompted for the new LAN IPv4 address. For the purpose of the tutorial I have used 192.168.0.254(pictured below).

To proceed: Type the **LAN IP** you will use then press **ENTER**

```
 WAN (wan)       -> em1        -> v4/DHCP4: 192.168.1.105/24
 LAN (lan)       -> em0        ->
 0) Logout (SSH only)                   9) pfTop
 1) Assign Interfaces                  10) Filter Logs
 2) Set interface(s) IP address        11) Restart webConfigurator
 3) Reset webConfigurator password     12) pfSense Developer Shell
 4) Reset to factory defaults          13) Upgrade from console
 5) Reboot system                      14) Enable Secure Shell (sshd)
 6) Halt system                        15) Restore recent configuration
 7) Ping host                          16) Restart PHP-FPM
 8) Shell


Enter an option: 2

Available interfaces:

1 - WAN (em1 - dhcp, dhcp6)
2 - LAN (em0 - static)

Enter the number of the interface you wish to configure: 2

Enter the new LAN IPv4 address.  Press <ENTER> for none:
> 192.168.0.254
```

Next you will be asked to provide a ***Subnet mask*** bit count in **CIDR** notation. This will almost **ALWAYS** be **24** for a local network.

To proceed: Type **24** then press **ENTER**

```
 5) Reboot system                    14) Enable Secure Shell (sshd)
 6) Halt system                      15) Restore recent configuration
 7) Ping host                        16) Restart PHP-FPM
 8) Shell


Enter an option: 2

Available interfaces:

1 - WAN (em1 - dhcp, dhcp6)
2 - LAN (em0 - static)

Enter the number of the interface you wish to configure: 2

Enter the new LAN IPv4 address.  Press <ENTER> for none:
> 192.168.0.254

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new LAN IPv4 subnet bit count (1 to 31):
> 24
```

The next few prompts can be skipped by pressing **ENTER** which indicates **NO SELECTION**(pictured below).

To proceed: press **ENTER**

```
Enter an option: 2

Available interfaces:

1 - WAN (em1 - dhcp, dhcp6)
2 - LAN (em0 - static)

Enter the number of the interface you wish to configure: 2

Enter the new LAN IPv4 address.  Press <ENTER> for none:
> 192.168.0.254

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new LAN IPv4 subnet bit count (1 to 31):
> 24

For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>
```

You will NOT need IPv6 configured(pictured below) on your LAN so this step can be skipped.

To proceed: press **ENTER**

```
Available interfaces:

1 - WAN (em1 - dhcp, dhcp6)
2 - LAN (em0 - static)

Enter the number of the interface you wish to configure: 2

Enter the new LAN IPv4 address.  Press <ENTER> for none:
> 192.168.0.254

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new LAN IPv4 subnet bit count (1 to 31):
> 24

For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Enter the new LAN IPv6 address.  Press <ENTER> for none:
>
```

To make the console configuration as simple as possible we will **NOT** enable **DHCP** on the **LAN** at this time(pictured below). That will be setup using the web interface.

To proceed: Type **n** then press **ENTER**

```
1 - WAN (em1 - dhcp, dhcp6)
2 - LAN (em0 - static)

Enter the number of the interface you wish to configure: 2

Enter the new LAN IPv4 address.  Press <ENTER> for none:
> 192.168.0.254

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new LAN IPv4 subnet bit count (1 to 31):
> 24

For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Enter the new LAN IPv6 address.  Press <ENTER> for none:
>

Do you want to enable the DHCP server on LAN? (y/n)
```

You will now be prompted to revert the web interface(pictured below) from secure(https) to non-secure(http). You may wish to leave it set to secure.

To proceed: Type **n** then press **ENTER**

```
2 - LAN (em0 - static)

Enter the number of the interface you wish to configure: 2

Enter the new LAN IPv4 address.  Press <ENTER> for none:
> 192.168.0.254

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new LAN IPv4 subnet bit count (1 to 31):
> 24

For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Enter the new LAN IPv6 address.  Press <ENTER> for none:
>

Do you want to enable the DHCP server on LAN? (y/n) n
Disabling IPv4 DHCPD...
Do you want to revert to HTTP as the webConfigurator protocol? (y/n)
```

The configuration should now be complete.

To proceed: press **ENTER**

```
Enter the new LAN IPv4 subnet bit count (1 to 31):
> 24

For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Enter the new LAN IPv6 address.  Press <ENTER> for none:
>

Do you want to enable the DHCP server on LAN? (y/n) n
Disabling IPv4 DHCPD...
Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n

Please wait while the changes are saved to LAN...
 Reloading filter...
 Reloading routing configuration...
 DHCPD...

The IPv4 LAN address has been set to 192.168.0.254/24
You can now access the webConfigurator by opening the following URL in your web
browser:
                https://192.168.0.254/

Press <ENTER> to continue.
```

2.4-Reset Admin Password

At some point you may wish to default the Admin credentials. The menu option is number 3(pictured below).

```
 Reloading routing configuration...
 DHCPD...

The IPv4 LAN address has been set to 192.168.0.254/24
You can now access the webConfigurator by opening the following URL in your web
browser:
                https://192.168.0.254/

Press <ENTER> to continue.
*** Welcome to pfSense 2.2.4-RELEASE-pfSense (amd64) on pfSense ***

 WAN (wan)       -> em1        -> v4/DHCP4: 192.168.1.105/24
 LAN (lan)       -> em0        -> v4: 192.168.0.254/24
 0) Logout (SSH only)                  9) pfTop
 1) Assign Interfaces                 10) Filter Logs
 2) Set interface(s) IP address       11) Restart webConfigurator
 3) Reset webConfigurator password    12) pfSense Developer Shell
 4) Reset to factory defaults         13) Upgrade from console
 5) Reboot system                     14) Enable Secure Shell (sshd)
 6) Halt system                       15) Restore recent configuration
 7) Ping host                         16) Restart PHP-FPM
 8) Shell


Enter an option:
```

If you select option **3** and press **y** indicating **YES** the credentials will be reset. The defaults are:

Username: **admin**

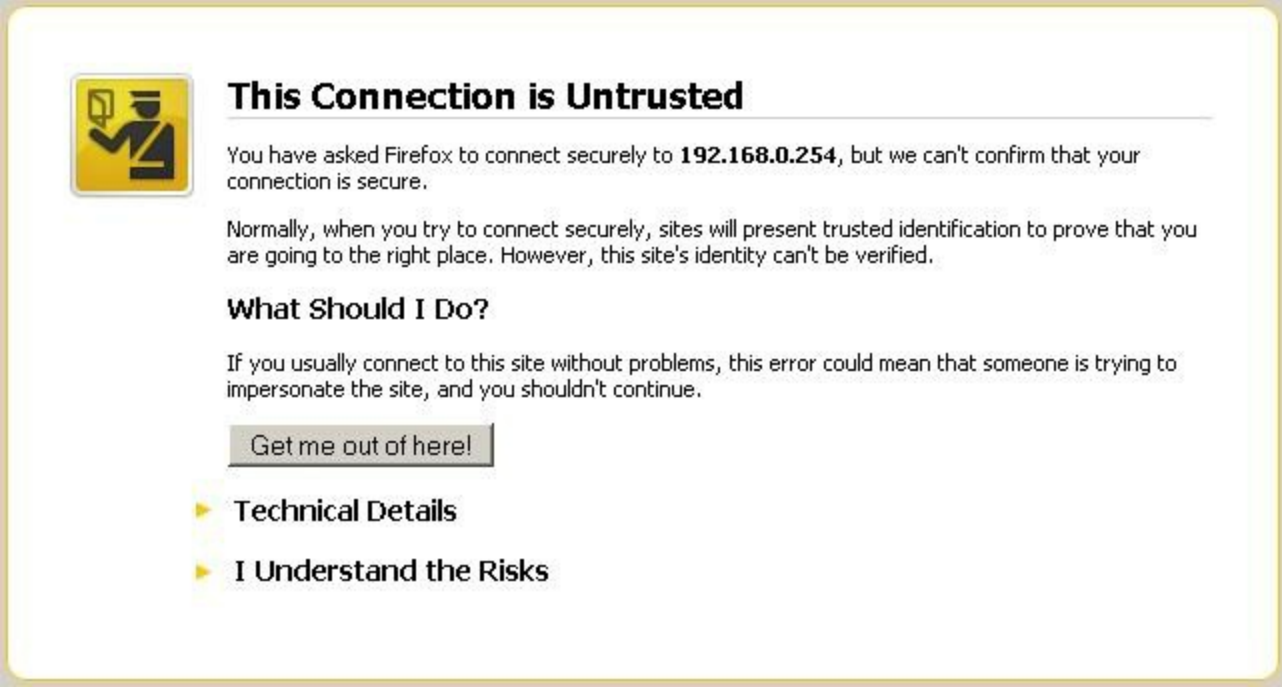
Password: **pfsense**

```
The webConfigurator admin password and privileges will be reset to the default (
which is "pfsense").
Do you want to proceed [y|n]?n
*** Welcome to pfSense 2.2.4-RELEASE-pfSense (amd64) on pfSense ***

 WAN (wan)       -> em1        -> v4/DHCP4: 192.168.1.105/24
 LAN (lan)       -> em0        -> v4: 192.168.0.254/24
 0) Logout (SSH only)                  9) pfTop
 1) Assign Interfaces                 10) Filter Logs
 2) Set interface(s) IP address       11) Restart webConfigurator
 3) Reset webConfigurator password    12) pfSense Developer Shell
 4) Reset to factory defaults         13) Upgrade from console
 5) Reboot system                     14) Enable Secure Shell (sshd)
 6) Halt system                       15) Restore recent configuration
 7) Ping host                         16) Restart PHP-FPM
 8) Shell


Enter an option: 3



The webConfigurator admin password and privileges will be reset to the default (
which is "pfsense").
Do you want to proceed [y|n]?
```

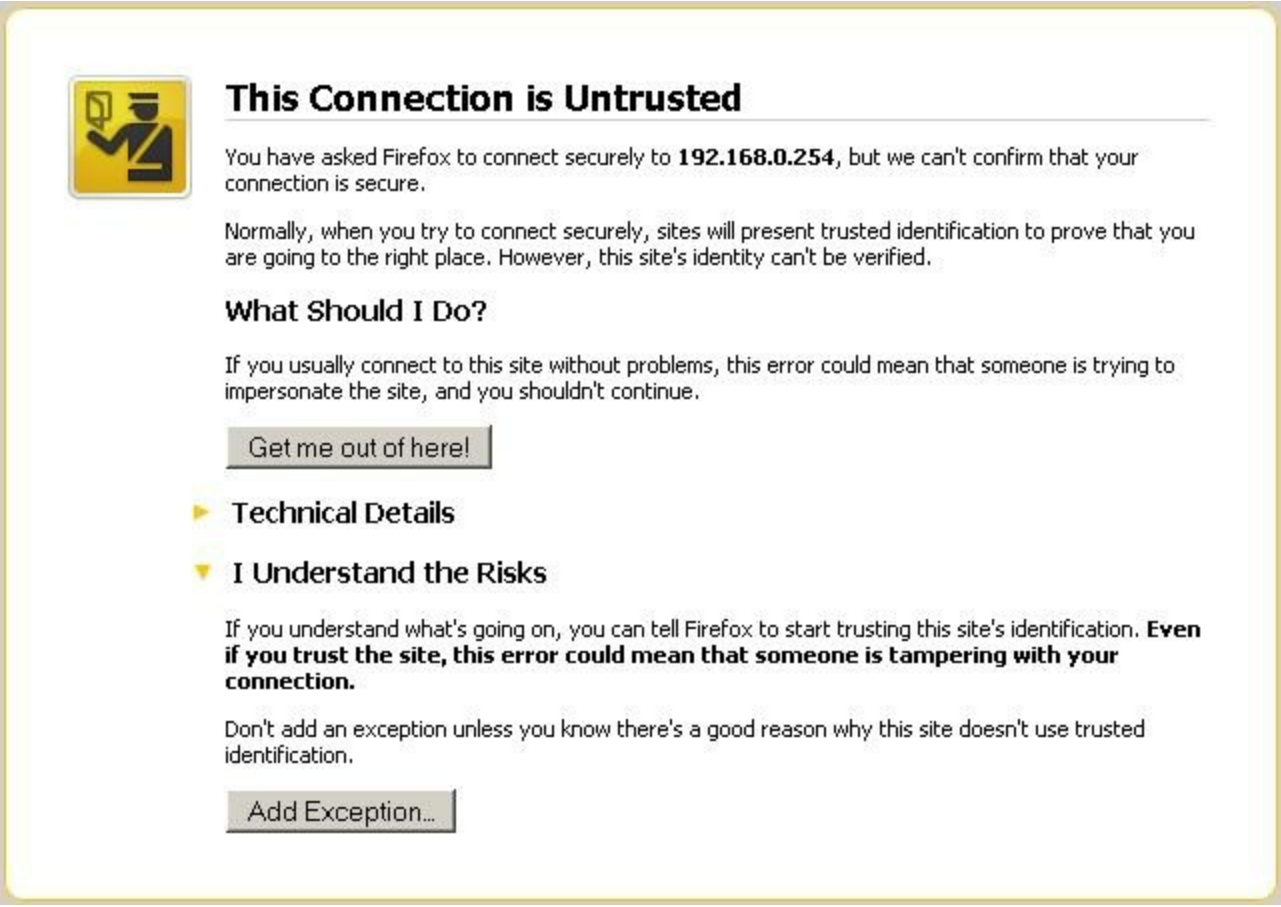
2.5-Web Configuration Wizard

You are now ready to open your web browser to the LAN address you just set(https://192.168.0.254) for a first login. For the purpose of this tutorial I have used Mozilla Firefox.

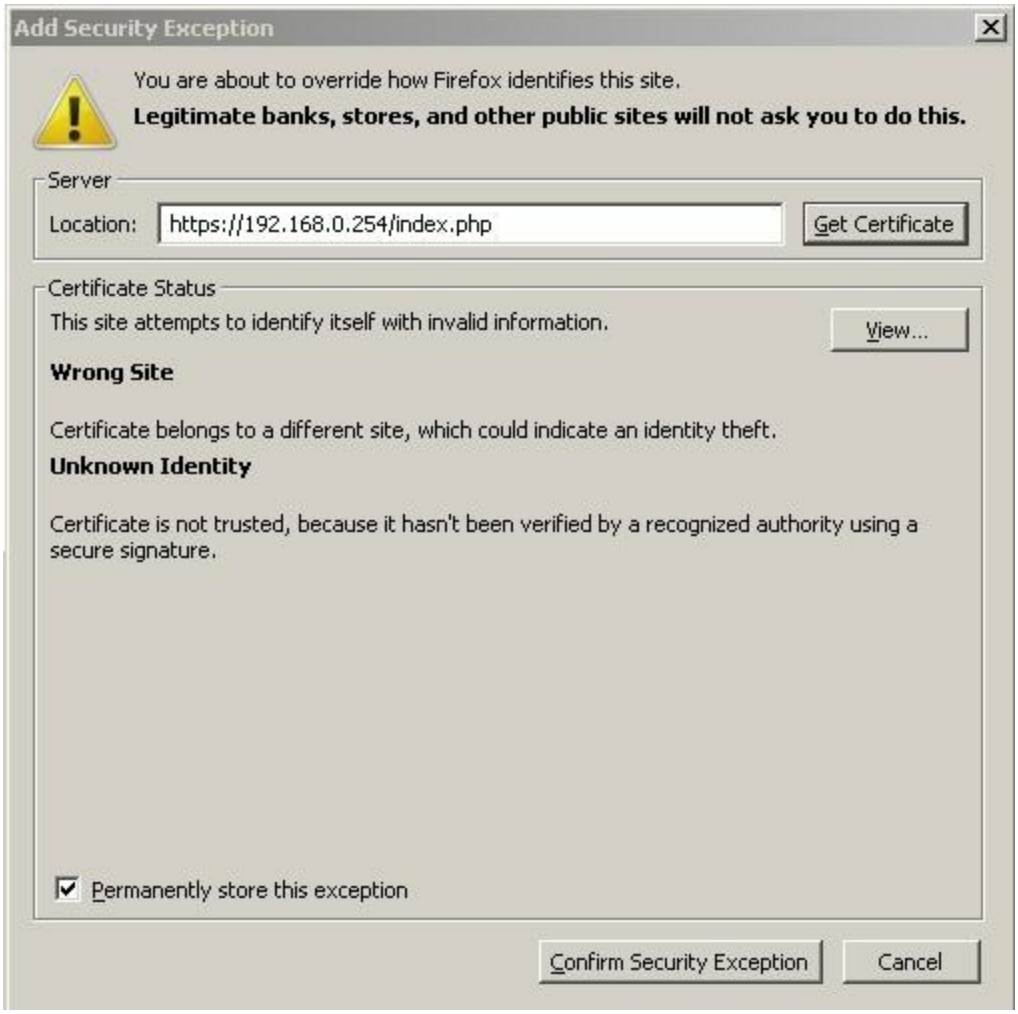
To continue(pictured below): click **I Understand the Risks**



Next(pictured below): click **Add Exception**



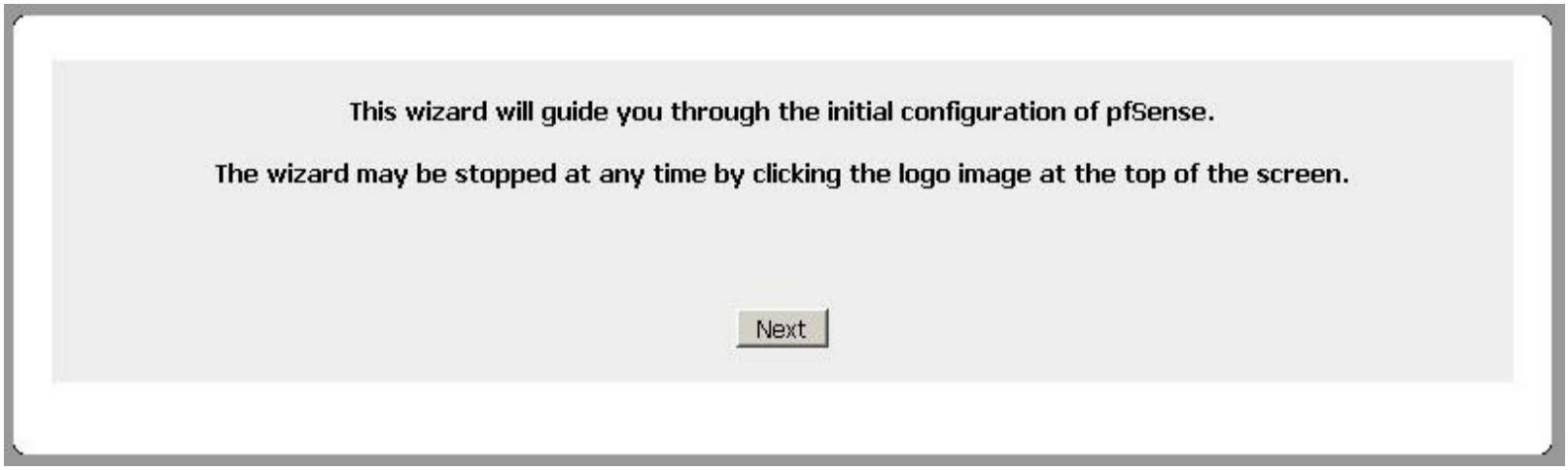
Now(pictured below): click **Confirm Security Exception**



To proceed: login(pictured below) using the default password: pfsense

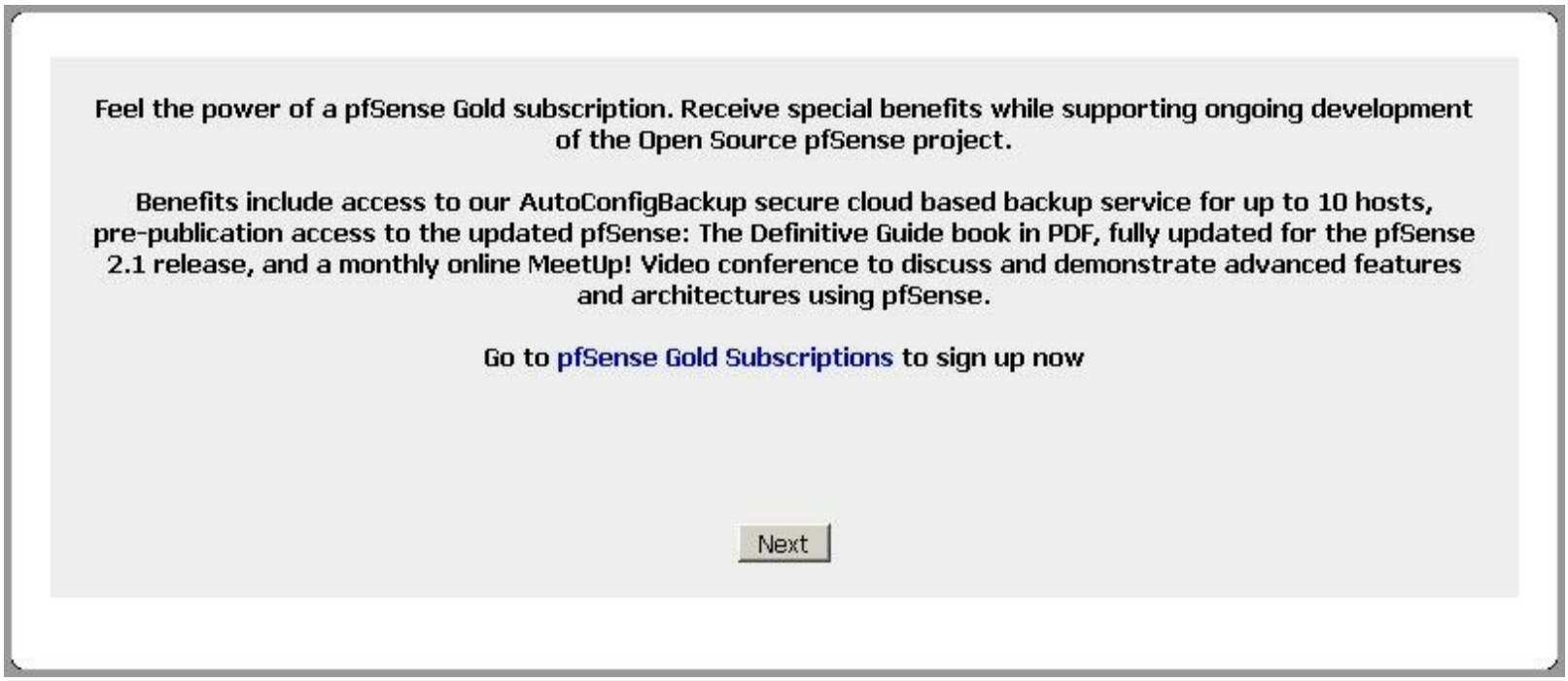
Once logged in the wizard will start(pictured below). Simply follow the prompts.

To proceed: click **Next**



pfSense now offers **Gold Subscription** signup(pictured below). This is **NOT** required in any way to use the software.

To proceed: click **Next**

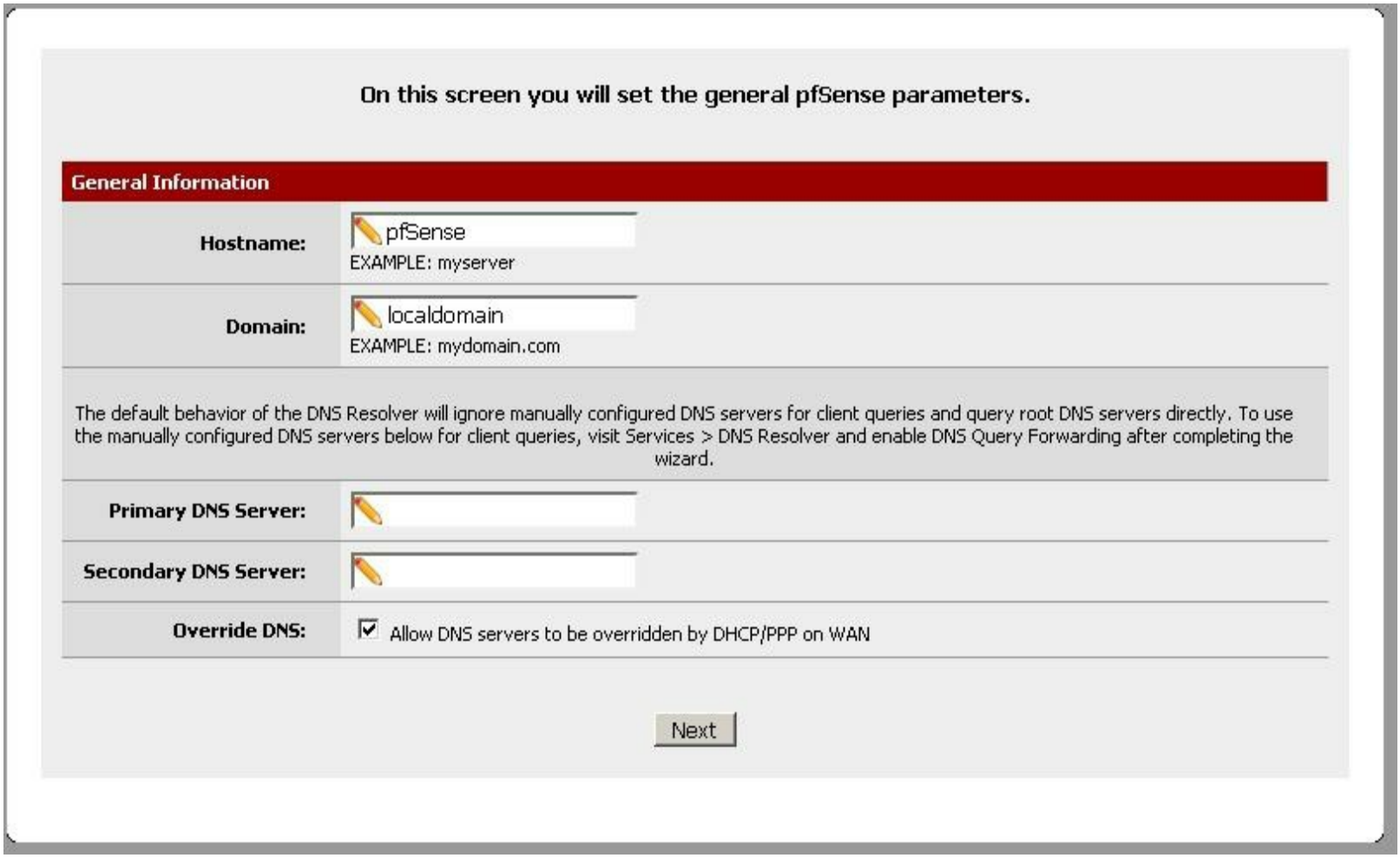


You will now be prompted to enter some basic information about your router(pictured below). To specify a **.com** domain other than **localdomain** or **YOURWEBS** you **MUST** have a registrar such as **Go Daddy**.

For example: I have a registered **YOURWEBS.US** domain so I can enter that below. If I didn't have that domain registered I could still use **YOURWEBS** leaving off the **.US** suffix. This will work just fine with my local **Zentyal** domain controller install. Regardless what name you choose, the domain entry should **match** that of the **Zentyal** controller we'll be setting up later in the book. My preference here is to **register** a domain that will **NOT** be used by the ***public*** but that still resolves to my **WAN** IP address.

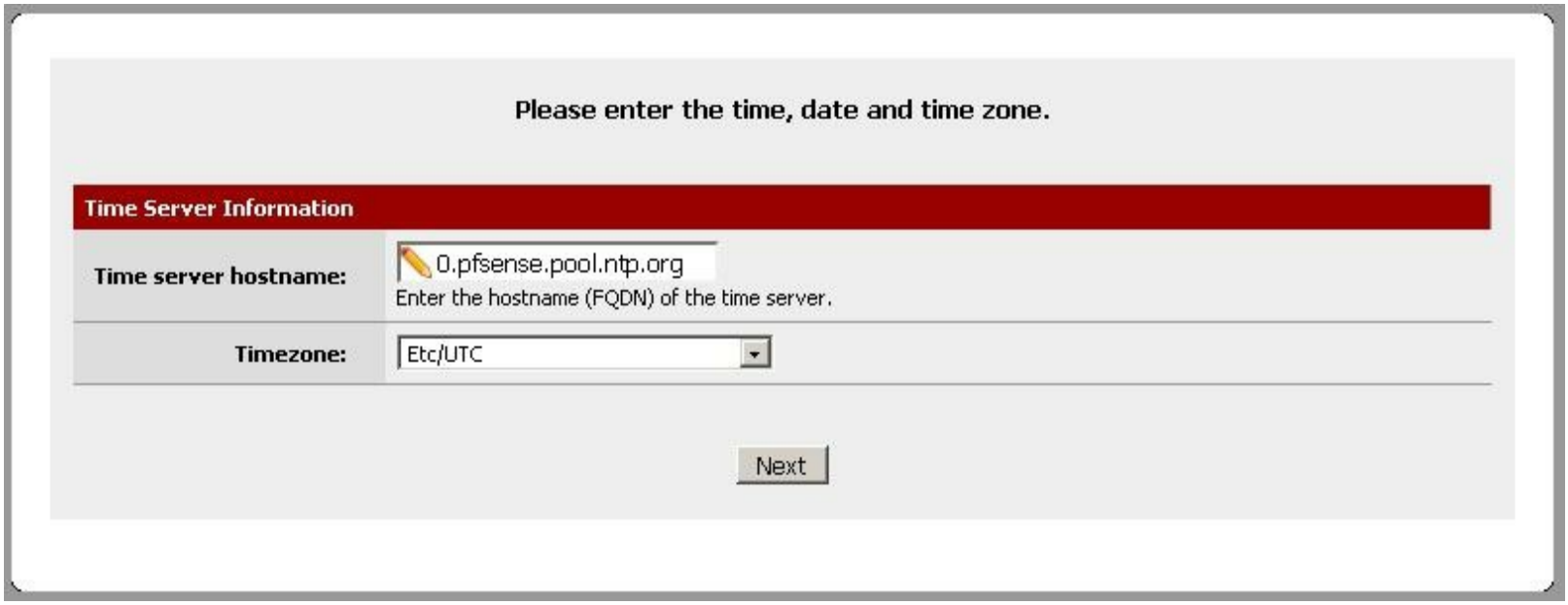
You may also wish to use **Google DNS** servers(8.8.8.8 and 8.8.4.4) as ***alternates*** instead of your ISP. This option can sometimes solve name resolution issues.

To proceed: click **Next**

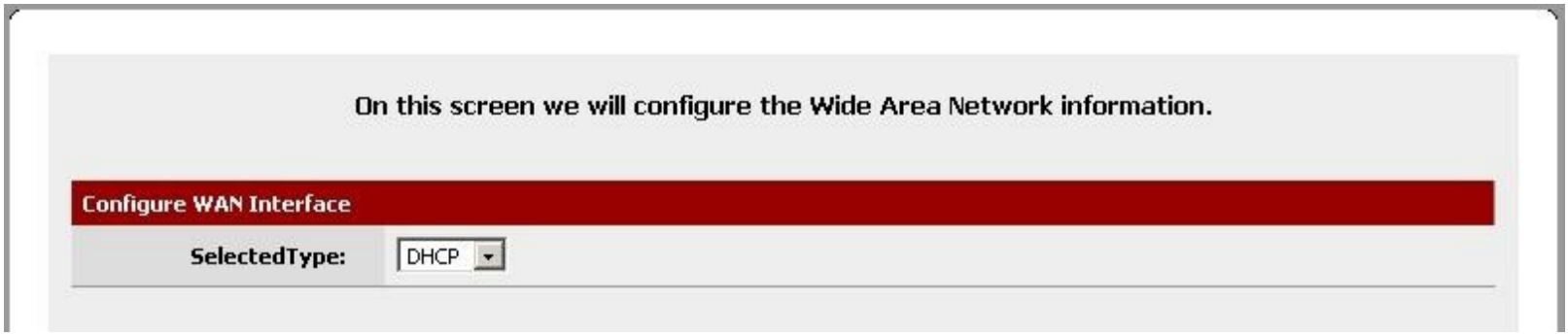


Now enter your Time server(recommend default) and Timezone information(pictured below).

To proceed: click **Next**

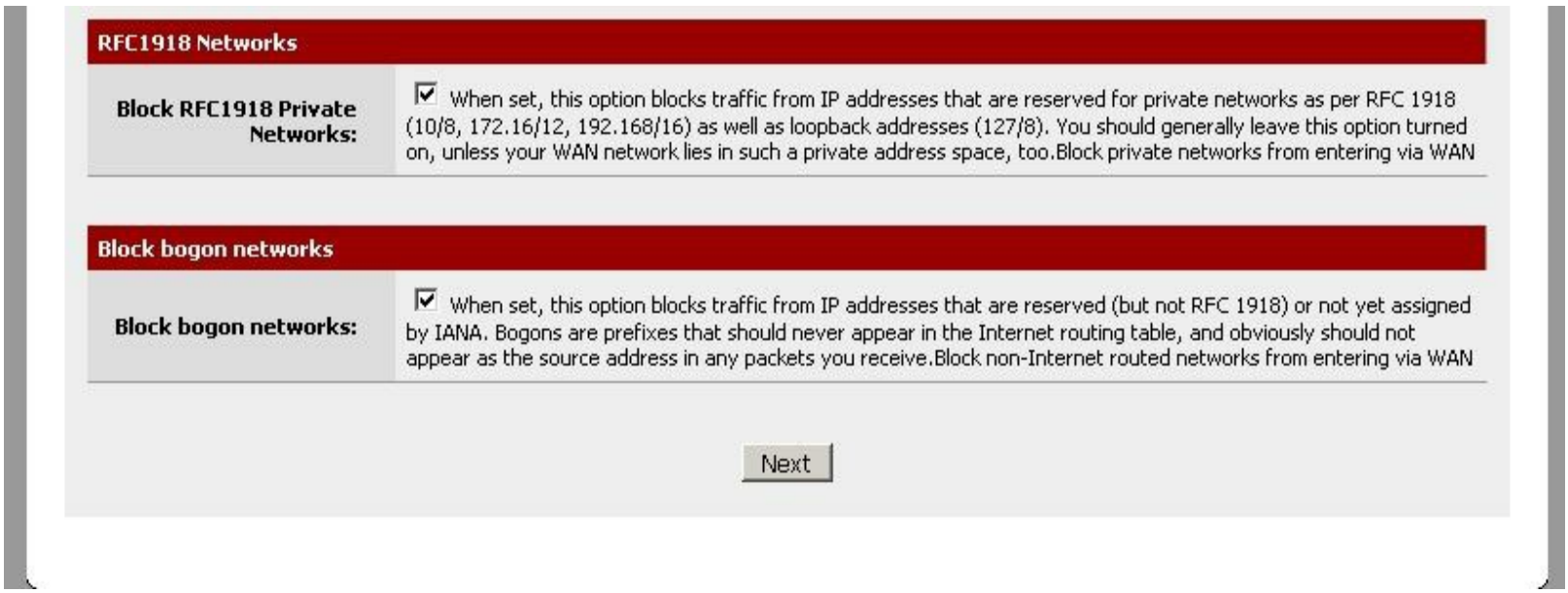


Since the **WAN** was already configured earlier this is redundant. It should almost **ALWAYS** be configured for **DHCP** (pictured below) with most ISP's today.



Scrolling down to the bottom of the screen reveals the following options(pictured below). You want both of these checked for **WAN** interfaces.

To proceed: click **Next**



Since we have already configured the LAN interface this step is again redundant. The values(pictured below) should match those you entered during the console stage of installation.

To proceed: click **Next**

On this screen we will configure the Local Area Network information.

Configure LAN Interface

LAN IP Address:	192.168.0.254 Type dhcp if this interface uses DHCP to obtain its IP address.
Subnet Mask:	24

Next

Next you will change the default **Admin Password**(pictured below) to a more secure one(make sure to do this).

To proceed: click **Next**

On this screen we will set the admin password, which is used to access the WebGUI and also SSH services if you wish to enable them.

Set Admin WebGUI Password

Admin Password:	●●●●●●●
Admin Password AGAIN:	●●●●●●●

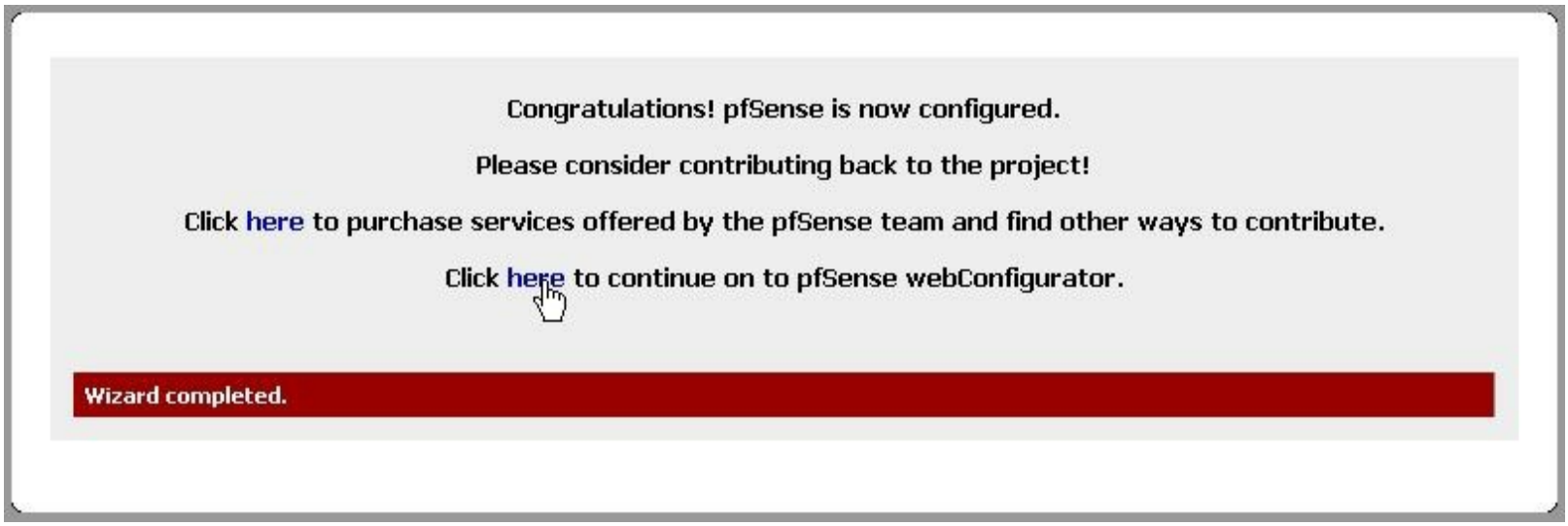
Next

Now, pfSense will reload the configuration changes(pictured below).

To proceed: click **Reload**

Congratulations! You are done with the initial setup.

To proceed: click the **here** link as **pictured below**



2.6-Changing Themes

The default theme and dashboard will look something like the picture shown below. Notice that everything is left justified. My preference is to change this to center justified for easier navigation and mobile phone compatibility.

https://192.168.0.254/index.php

Google

pfSense | System | Interfaces | Firewall | Services | VPN | Status | Diagnostics | Gold | Help | pfSense.localdomain

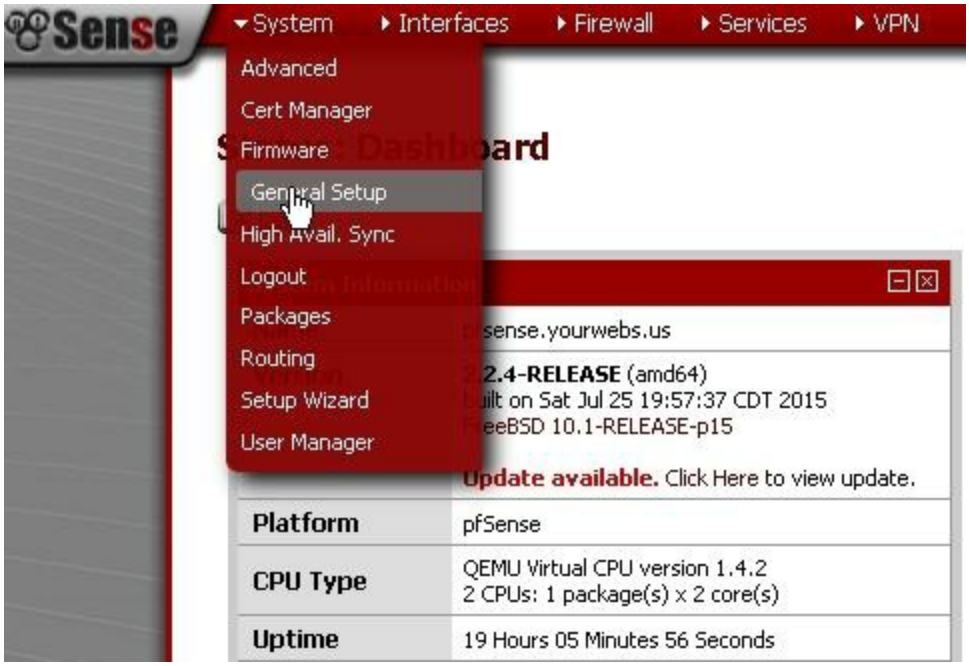
Status: Dashboard

System Information	
Name	pfSense.localdomain
Version	**2.2.4-RELEASE** (amd64) built on Sat Jul 25 19:57:37 CDT 2015 FreeBSD 10.1-RELEASE-p15 Unable to check for updates.
Platform	pfSense
CPU Type	QEMU Virtual CPU version 1.4.2
Uptime	00 Hour 49 Minutes 43 Seconds
Current date/time	Tue Dec 1 15:42:02 CST 2015
DNS server(s)	127.0.0.1 192.168.1.1
Last config change	Tue Dec 1 15:34:23 CST 2015
State table size	0% (60/47000) Show states
MBUF Usage	3% (760/26584)
Load average	0.07, 0.15, 0.07
CPU usage	0%
Memory usage	22% of 477 MB
SWAP usage	0% of 1023 MB
Disk usage	/ (ufs): 6% of 6.8G /var/run (ufs in RAM): 4% of 3.4M

Interfaces		
WAN (DHCP)	↑	1000baseT <full-duplex> **0.0.0.0**
LAN	↑	1000baseT <full-duplex> **192.168.0.254**

pfSense is © 2004 - 2015 by Electric Sheep Fencing LLC. All Rights Reserved. [view license]

Let's change the default theme to **NERVECENTER** by selecting **System>General Setup** as shown below.



Now scroll to the bottom and select the **NERVCENTER** theme from the dropdown list(pictured below). Don't forget to save the changes!

Your new NERVCENTER theme should look something like this(pictured below).

192.168.0.254/index.php

pfSense

pfsense.yourwebs.us

System Interfaces Firewall Services VPN Status Diagnostics Gold Help

Status: Dashboard

System Information

Name	pfsense.yourwebs.us
Version	**2.2.4-RELEASE** (amd64) built on Sat Jul 25 19:57:37 CDT 2015 FreeBSD 10.1-RELEASE-p15 **Update available.** Click Here to view update.
Platform	pfSense
CPU Type	QEMU Virtual CPU version 1.4.2 2 CPUs: 1 package(s) x 2 core(s)
Uptime	19 Hours 15 Minutes 15 Seconds
Current date/time	Tue Dec 8 14:25:37 CST 2015
DNS server(s)	127.0.0.1 8.8.8.8 8.8.4.4
Last config change	Tue Dec 8 14:24:16 CST 2015
State table size	0% (257/815000) Show states
MBUF Usage	6% (1526/26584)
Load average	0.12, 0.12, 0.10
CPU usage	1%
Memory usage	3% of 8157 MB
Disk usage	/ (ufs): 16% of 3.9G /tmp (ufs in RAM): 1% of 38M /var (ufs in RAM): 46% of 58M

Snort Alerts

IF/Date	Src/Dst Address	Description
LAN Dec 08 06:46:46	152.163.13.67:80 192.168.0.41:50122	(http_inspect) MULTIPLE ENCODINGS WITHIN

Interfaces

SPRINT (DHCP)	↑	1000baseT <full-duplex> 192.168.2.103
LAN	↑	1000baseT <full-duplex> 192.168.0.254
DMZ	↑	1000baseT <full-duplex> 192.168.5.254
JAB (DHCP)	↑	100baseTX <full-duplex> 206.248.44.213

Interface Statistics

	SPRINT	LAN	DMZ	JAB
Packets In	369739	3490612	69709	6271335
Packets Out	276603	6501680	82595	3393971
Bytes In	381.74 MB	236.03 MB	23.22 MB	7.61 GB
Bytes Out	25.19 MB	7.93 GB	69.20 MB	240.80 MB
Errors In	0	0	0	0
Errors Out	0	0	0	0
Collisions	0	0	0	0

OpenVPN

SkybeamVPN UDP:1194 Client connections

Name/Time	Real/Virtual IP

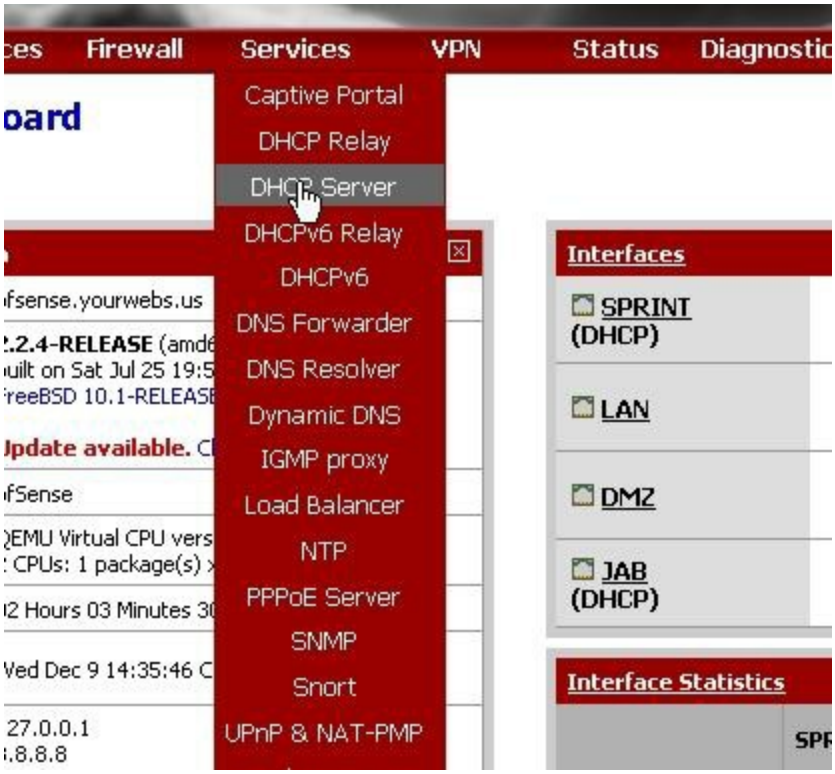
Gateways

Name	RTT	Loss	Status
JAB_DHCP	206.248.44.1		
	62.1ms	0%	Online
SPRINT_DHCP	192.168.2.254		
	38ms	100%	Offline

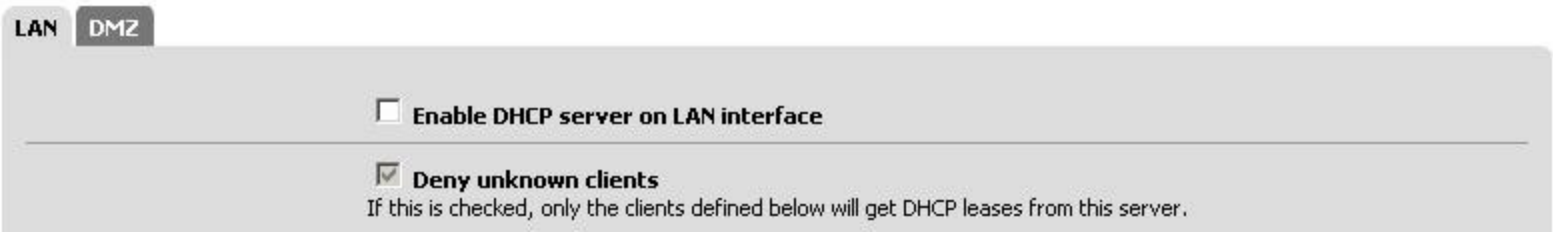
2.7-Configure DHCP Server

The next step is to enable the DHCP server on the LAN. This will assign IP addresses to any machine connected locally.

To proceed: click **Services>DHCP Server** as pictured below.



You should see the following window(shown below). Check the box: **Enable DHCP server on LAN interface**



Once the service box is checked you will need to set a **range**(pictured below). My preference is to use a **range** (x.x.x.100-x.x.x.200). This allows for static reservation addressing before and after the range which is very useful. Also notice the ***Deny unknown clients switch***(pictured below). I prefer to keep this unchecked until all entries are added to the system. Once everything is verified and working you can check this box and save changes. This will prevent unauthorized hardware from obtaining addresses on your system(***very useful and highly recommended***).

LAN DMZ

	☑ **Enable DHCP server on LAN interface**
	☐ **Deny unknown clients** If this is checked, only the clients defined below will get DHCP leases from this server.
Subnet	192.168.0.0
Subnet mask	255.255.255.0
Available range	192.168.0.1 - 192.168.0.254
Range	192.168.0.100 to 192.168.0.200

2.7.1-WINS, DNS, Gateway, and Domain

When a ***client*** connects to the **DHCP** server it receives all the information from the following entries. In this example we will be installing **Zentyal** to act as a directory server for the **YOURWEBS.US** domain. The **WINS servers** entries below are the addresses of **ZentyalDC1** and **ZentyalDC2** respectively. The **DNS** and **Gateway** entries are the **pfSense** LAN interface IP.

WINS servers	192.168.0.75 192.168.0.76
DNS servers	192.168.0.254 NOTE: leave blank to use the system default DNS servers - this interface's IP if DNS Forwarder or Resolver is enabled, otherwise the servers configured on the General page.
Gateway	192.168.0.254 The default is to use the IP on this interface of the firewall as the gateway. Specify an alternate gateway here if this is not the correct gateway for your network. Type "none" for no gateway assignment.
Domain name	yourwebs.us The default is to use the domain name of this system as the default domain name provided by DHCP. You may specify an alternate domain name here.
Domain search list	yourwebs.us The DHCP server can optionally provide a domain search list. Use the semicolon character as separator

The picture below shows another security switch that I prefer to keep turned off until everything is verified to be working. By **Enabling Static ARP Entries** pfSense will prevent **ANY** hardware **NOT** listed from communicating with the **LAN** adapter. This is yet another powerful tool to help keep your network secure(***strongly recommended***)!

Static ARP	☐ **Enable Static ARP entries** **Note:** This option persists even if DHCP server is disabled. Only the machines listed below will be able to communicate with the firewall on this NIC.

2.7.2-DHCP Client Reservations

If you scroll to the bottom of the page you will see the Static mappings table. The one pictured below is ***pre-populated*** to give you an idea what the table will look like after making a few entries. I strongly recommend entering **EVERY** hardware address in your network here with full descriptions(as shown below). Not only is it **necessary** if you wish to enable **static ARP entries**(shown above), but it comes in handy if you need to quickly look up the IP address of any machine on your network.

To make an entry: click the **+ button** on the right side(shown below).

DHCP Static Mappings for this interface.

Static ARP	MAC address	IP address	Hostname	Description
	92:26:b9:c2:42:14	192.168.0.3	Artica-PDC	ArticaNAS 1.8 Directory Server
	9a:09:d3:42:06:8b	192.168.0.4	NAS4Free1	NAS4Free1 on Proxmox2
	00:23:ae:7f:91:5a	192.168.0.5	FreeNAS-Backup	FreeNAS Optiplex 360 Backup Server
	08:62:66:29:59:cd	192.168.0.7	Proxmox2	Proxmox 2 eth2 vmbr0
	22:7c:29:db:16:3c	192.168.0.9	freeNAS-1-eth1	freeNAS-1 iscsi interface
	7a:a9:6c:6a:30:8d	192.168.0.10	freenas-1	FreeNAS Primary
	7a:a9:6c:6a:30:8e	192.168.0.11	freenas-2	FreeNAS Secondary
	2a:7a:4b:d7:7b:97	192.168.0.13	mythbuntu	Virtual Media Server

Next you should see the DHCP entry form(shown below). I have included a sample entry for reference(shown below). After making an entry be sure to save your changes. **NOTE**: There is really **NO** need to make WINS, DNS, Gateway, or any other entries here. By default the **pfSense interface IP** will control **ALL** clients automatically.

Static DHCP Mapping on LAN

MAC address	50:e5:49:e5:c5:c5 Copy my MAC address Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx
Client identifier	
IP address	192.168.0.72 If an IPv4 address is entered, the address must be outside of the pool. If no IPv4 address is given, one will be dynamically allocated from the pool.
Hostname	vhost2 Name of the host, without domain part.
Description	sample dhcp entry You may enter a description here for your reference (not parsed).
ARP Table Static Entry	☑ Create an ARP Table Static Entry for this MAC & IP Address pair.
WINS servers	
DNS servers	NOTE: leave blank to use the system default DNS servers - this interface's IP if DNS Forwarder or Resolver is enabled, otherwise the servers configured on the General page.
Gateway	The default is to use the IP on this interface of the firewall as the gateway. Specify an alternate gateway here if this is not the correct gateway for your network.
Domain name	The default is to use the domain name of this system as the default domain name provided by DHCP. You may specify an alternate domain name here.
Domain search list	The DHCP server can optionally provide a domain search list. Use the semicolon character as separator
Default lease time	seconds This is used for clients that do not ask for a specific expiration time. The default is 7200 seconds.
Maximum lease time	seconds This is the maximum lease time for clients that ask for a specific expiration time. The default is 86400 seconds.
Dynamic DNS	Advanced - Show Dynamic DNS
NTP servers	Advanced - Show NTP configuration
TFTP server	Advanced - Show TFTP configuration

Save Cancel

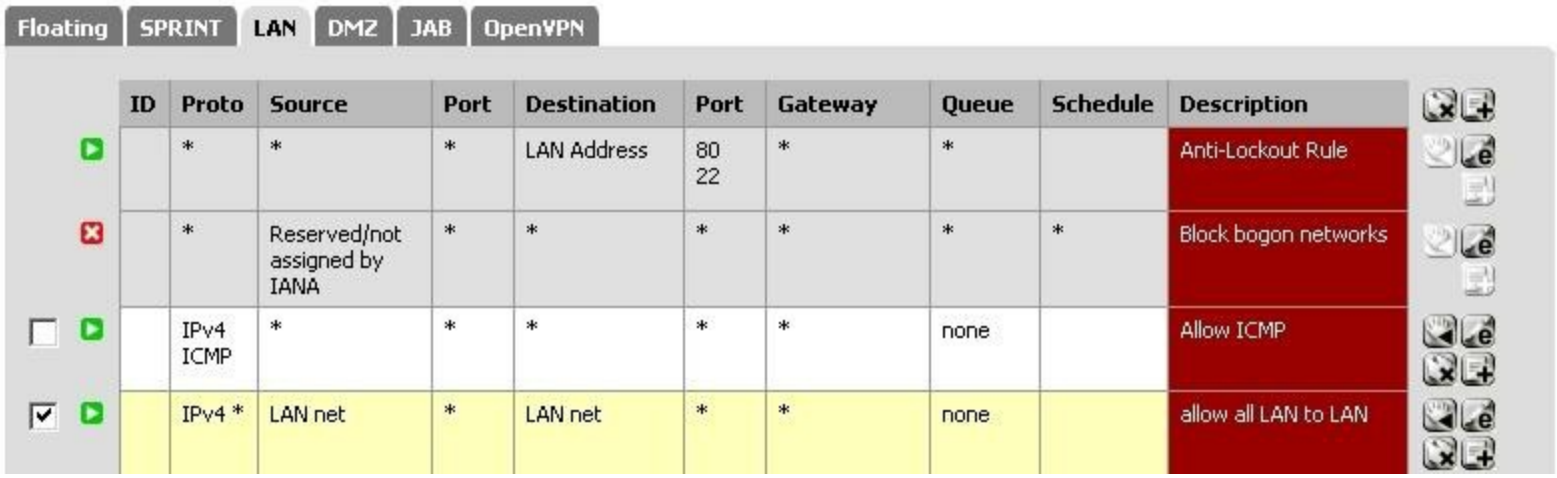
2.8-Firewall Settings

The last thing you'll need to do is setup a couple firewall rules. We will allow ALL traffic between LAN clients and allow ALL LAN clients out on the WAN. First we'll add the LAN to LAN rule.

To proceed: click **Firewall>Rules** as shown below

2.8.1-LAN Rules

You should see tabs with the names of your network interfaces. Some of my tabs(pictured below) have ***different names***. I have simply renamed them! For Example: I have renamed my **WAN** interface to **JAB**. The only interfaces we're going to concern with for this book are **LAN** and **WAN**. The list pictured below is ***pre-populated*** to give you an idea what the table will look like after making our LAN Rule entry.



ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
	*	*	*	LAN Address	80 22	*	*		Anti-Lockout Rule
	*	Reserved/not assigned by IANA	*	*	*	*	*	*	Block bogon networks
	IPv4 ICMP	*	*	*	*	*	none		Allow ICMP
	IPv4 *	LAN net	*	LAN net	*	*	none		allow all LAN to LAN

To add our new **LAN to LAN** rule click the **+ button** on the right side(pictured below).

Floating | SPRINT | LAN | DMZ | JAB | OpenVPN

	ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
		*	*	*	LAN Address	80 22	*	*		Anti-Lockout Rule
		*	Reserved/not assigned by IANA	*	*	*	*	*	*	Block bogon networks

The picture below shows the completed **LAN to LAN** rule. Duplicate this rule remembering to save the changes when finished.

Edit Firewall rule

Action	Pass Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.
Disabled	☐ **Disable this rule** Set this option to disable this rule without removing it from the list.
Interface	LAN Choose which interface packets must be sourced on to match this rule.
TCP/IP Version	IPv4 **Select the Internet Protocol version this rule applies to**
Protocol	any Choose which IP protocol this rule should match. Hint: in most cases, you should specify *TCP* here.
Source	☐ **not** Use this option to invert the sense of the match. Type: LAN net Address: / 127
Destination	☐ **not** Use this option to invert the sense of the match. Type: LAN net Address: / 127
Log	☐ **Log packets that are handled by this rule** Hint: the firewall has limited local log space. Don't turn on logging for everything. If you want to do a lot of logging, consider using a remote syslog server (see the Diagnostics: System logs: Settings page).
Description	allow all LAN to LAN You may enter a description here for your reference.

Save | Cancel

2.8.2-WAN Rules

Next we'll setup a rule allowing all **LAN** outbound on the **WAN**. Remember, I have renamed my **WAN** interface to **JAB**(pictured below)! The entry on your system will be made under the **WAN** tab.

The list pictured below is ***pre-populated*** to give you an idea what the table will look like after making our **WAN** Rule entry.

Floating | SPRINT | LAN | DMZ | JAB | OpenVPN

ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
	*	Reserved/not assigned by IANA	*	*	*	*	*	*	Block bogon networks
	IPv4 *	*	*	*	*	*	none		Block All
	IPv4 *	*	*	*	*	*	none		allow all temp
	IPv4 *	LAN net	*	*	*	*	none		Allow all LAN out

To add our new **LAN to ANY** rule click the **+ button** on the right side(pictured below).

Floating | SPRINT | LAN | DMZ | JAB | OpenVPN

ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
	*	Reserved/not assigned by IANA	*	*	*	*	*	*	Block bogon networks
	IPv4 *	*	*	*	*	*	none		Block All

The picture below shows the completed **LAN to ANY** rule on the **WAN** interface. Duplicate this rule remembering to save the changes when finished.

Edit Firewall rule

Action	Pass Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.
Disabled	☐ **Disable this rule** Set this option to disable this rule without removing it from the list.
Interface	JAB Choose which interface packets must be sourced on to match this rule.
TCP/IP Version	IPv4 **Select the Internet Protocol version this rule applies to**
Protocol	any Choose which IP protocol this rule should match. Hint: in most cases, you should specify *TCP* here.
Source	☐ **not** Use this option to invert the sense of the match. Type: LAN net Address: / 127
Destination	☐ **not** Use this option to invert the sense of the match. Type: any Address: / 127
Log	☐ **Log packets that are handled by this rule** Hint: the firewall has limited local log space. Don't turn on logging for everything. If you want to do a lot of logging, consider using a remote syslog server (see the Diagnostics: System logs: Settings page).
Description	Allow all LAN out You may enter a description here for your reference.

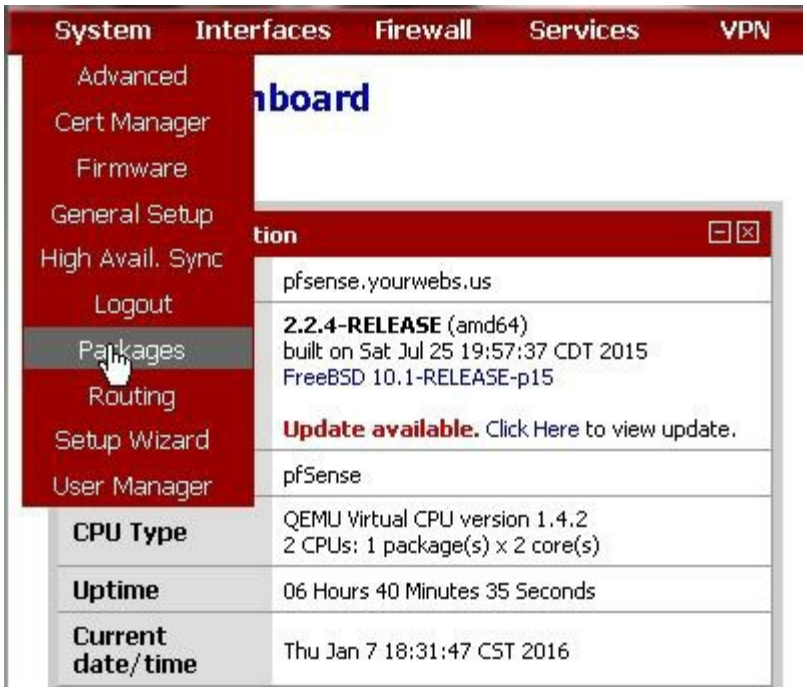
Save Cancel

2.9-OpenVPN

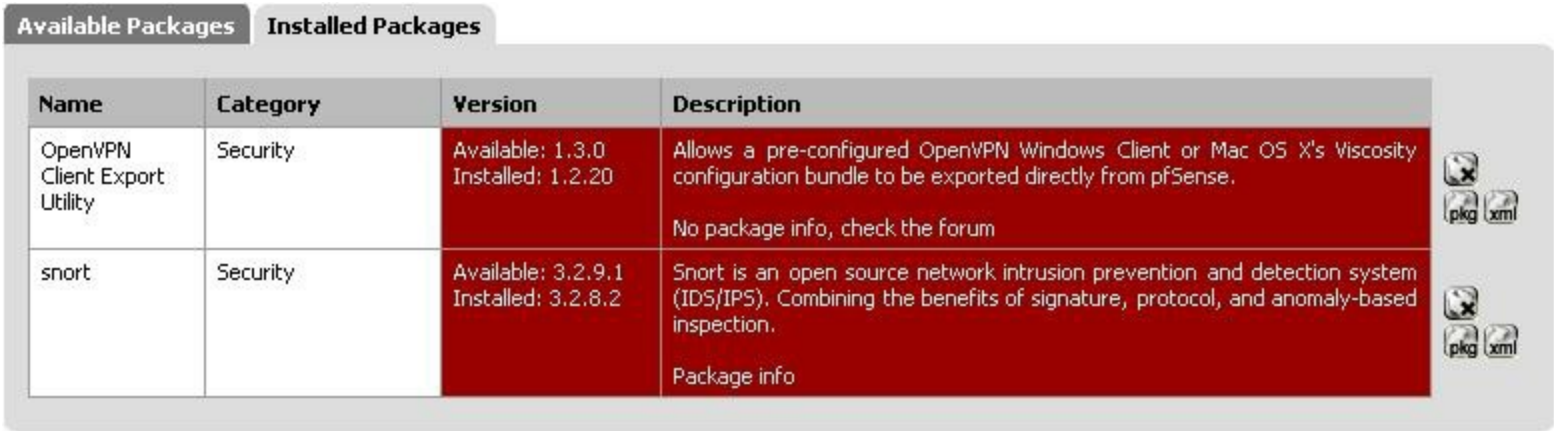
VPN is a tunneling protocol which allows secure remote access to your system. Once connected to the VPN tunnel clients can work as though they were onsite. In order for VPN to work you must have a static IP address and all remote machines must have a client connector installed. Configuring VPN manually can be quite challenging, even to professionals, but the pfSense developers have included a fantastic wizard to get you up and running with minimal effort. NOTE: even with the wizard this will be a lengthy chapter so better get your coffee and pay close attention! Let's get started!

2.9.1-OpenVPN Client Export Utility

To begin: click **System>Packages**(shown below).



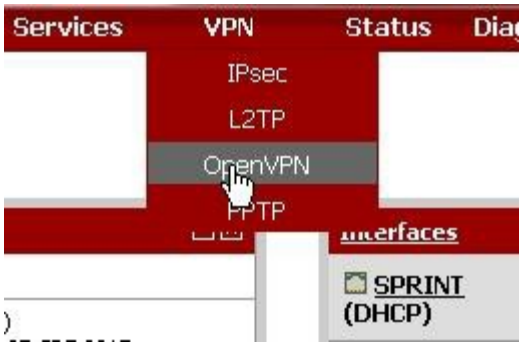
If you do not see ***OpenVPN Client Export Utility*** under **Installed Packages** download and install it under the **Available Packages** tab(pictured below).



2.9.2-OpenVPN Setup Wizard

Once the ***OpenVPN Client Export Utility*** is installed go to the main dashboard screen then click

VPN>OpenVPN(pictured below).



Next, click the Wizards tab(pictured below).

For now, select **Local User Access** from the dropdown then click the **Next** button(shown below).

You will now need to establish a **Certificate Authority** (CA). Complete the form as shown below then click **Add new CA**.

OpenVPN Remote Access Server Setup Wizard

Create a New Certificate Authority (CA) Certificate

Descriptive name:	LRS-TEK A name for your reference, to identify this certificate. This is the same as common-name field for other Certificates.
Key length:	1024 bit Size of the key which will be generated. The larger the key, the more security it offers, but larger keys are generally slower to use.
Lifetime:	3650 Lifetime in days. This is commonly set to 3650 (Approximately 10 years.)
Country Code:	us Two-letter ISO country code (e.g. US, AU, CA)
State or Province:	tx Full State or Province name, not abbreviated (e.g. Kentucky, Indiana, Ontario).
City:	alvarado City or other Locality name (e.g. Louisville, Indianapolis, Toronto).
Organization:	LRS-TEK Organization name, often the Company or Group name.
E-mail:	lee.surber@linuxsolutions.us E-mail address for the Certificate contact. Often the e-mail of the person generating the certificate (i.e. You.)

Add new CA

Next, you will need to create a ***New Server Certificate***. Keep the **Key length** at ***1024 bits*** for best results. When finished click **Create new Certificate**(pictured below).

OpenVPN Remote Access Server Setup Wizard

Create a New Server Certificate

Descriptive name:	vpncert A name for your reference, to identify this certificate. This is also known as the certificate's "Common Name."
Key length:	1024 bits Size of the key which will be generated. The larger the key, the more security it offers, but larger keys are generally slower to use.
Lifetime:	3650 Lifetime in days. This is commonly set to 3650 (Approximately 10 years.)
Country Code:	us Two-letter ISO country code (e.g. US, AU, CA)
State or Province:	tx Full State of Province name, not abbreviated (e.g. Kentucky, Indiana, Ontario).
City:	alvarado City or other Locality name (e.g. Louisville, Indianapolis, Toronto).
Organization:	LRS-TEK Organization name, often the Company or Group name.
E-mail:	lee.surber@linuxsolutions.us E-mail address for the Certificate contact. Often the e-mail of the person generating the certificate (i.e. You.)

Create new Certificate

In the ***General Information*** section below I have left **Protocol** and **Port** values at ***default***. The **Interface** should normally be **WAN** but I have renamed mine to **JAB** in this server. This helps for identification purposes when you have several WAN connections all hosting VPN tunnels.

OpenVPN Remote Access Server Setup Wizard

General OpenVPN Server Information	
Interface:	JAB The interface where OpenVPN will listen for incoming connections (typically WAN.)
Protocol:	UDP Protocol to use for OpenVPN connections. If you are unsure, leave this set to UDP.
Local Port:	1194 Local port upon which OpenVPN will listen for connections. The default port is 1194. This can be left at its default unless you need to use a different port.
Description:	JabVPN A name for this OpenVPN instance, for your reference. It can be set however you like, but is often used to distinguish the purpose of the service (e.g. "Remote Technical Staff"). It is also used by OpenVPN Client Export to identify this VPN on clients.

The ***Cryptographic Settings***(shown below) should also be left at ***default*** unless you know what you are doing.

Cryptographic Settings	
TLS Authentication:	☑ Enable authentication of TLS packets.
Generate TLS Key:	☑ Automatically generate a shared TLS authentication key.
TLS Shared Key:	Paste in a shared TLS key if one has already been generated.
DH Parameters Length:	1024 bit Length of Diffie-Hellman (DH) key exchange parameters, used for establishing a secure communications channel. As with other such settings, the larger values are more secure, but may be slower in operation.
Encryption Algorithm:	AES-128-CBC (128-bit) The algorithm used to encrypt traffic between endpoints. This setting must match on the client and server side, but is otherwise set however you like. Certain algorithms will perform better on different hardware, depending on the availability of supported VPN accelerator chips.
Auth Digest Algorithm:	SHA1 (160-bit) The method used to authenticate traffic between endpoints. This setting must match on the client and server side, but is otherwise set however you like.
Hardware Crypto:	No Hardware Crypto Acceleration The hardware cryptographic accelerator to use for this VPN connection, if any.

For ***Tunnel Settings***(shown below) I have allowed **1 client** in the 10.10.10.0/24 **Tunnel Network**. This client will have access to the 192.168.0.0/24 **Local Network**.

Tunnel Settings	
Tunnel Network:	10.10.10.0/24 This is the virtual network used for private communications between this server and client hosts expressed using CIDR notation (eg. 10.0.8.0/24). The first network address will be assigned to the server virtual interface. The remaining network addresses can optionally be assigned to connecting clients. (see Address Pool)
Redirect Gateway:	☐ Force all client generated traffic through the tunnel.
Local Network:	192.168.0.0/24 This is the network that will be accessible from the remote endpoint, expressed as a CIDR range. You may leave this blank if you don't want to add a route to the local network through this tunnel on the remote machine. This is generally set to your LAN network.
Concurrent Connections:	1 Specify the maximum number of clients allowed to concurrently connect to this server.
Compression:	No Preference Compress tunnel packets using the LZO algorithm. Adaptive compression will dynamically disable compression for a period of time if OpenVPN detects that the data in the packets is not being compressed efficiently.
Type-of-Service:	☑ Set the TOS IP header value of tunnel packets to match the encapsulated packet's TOS value.
Inter-Client Communication:	☐ Allow communication between clients connected to this server.
Duplicate Connections:	☐ Allow multiple concurrent connections from clients using the same Common Name. NOTE: This is not generally recommended, but may be needed for some scenarios.

In ***Client Settings***(pictured below) I have allowed **Dynamic IP** and **Address Pool**. I have also assigned the ***pfSense IP address*** as the **DNS Server** and supplied YOURWEBS.US as a **Default Domain**. When finished click **Next**(shown below).

Client Settings

Dynamic IP:	☑ Allow connected clients to retain their connections if their IP address changes.
Address Pool:	☑ Provide a virtual adapter IP address to clients (see Tunnel Network).
DNS Default Domain:	yourwebs.us Provide a default domain name to clients.
DNS Server 1:	192.168.0.254 DNS server IP to provide to connecting clients.
DNS Server 2:	DNS server IP to provide to connecting clients.
DNS Server 3:	DNS server IP to provide to connecting clients.
DNS Server 4:	DNS server IP to provide to connecting clients.
NTP Server:	Network Time Protocol server to provide to connecting clients.
NTP Server 2:	Network Time Protocol server to provide to connecting clients.
NetBIOS Options:	☐ Enable NetBIOS over TCP/IP. If this option is not set, all NetBIOS-over-TCP/IP options (including WINS) will be disabled.
NetBIOS Node Type:	none Possible options: b-node (broadcasts), p-node (point-to-point name queries to a WINS server), m-node (broadcast then query name server), and h-node (query name server, then broadcast).
NetBIOS Scope ID:	A NetBIOS Scope ID provides an extended naming service for NetBIOS over TCP/IP. The NetBIOS scope ID isolates NetBIOS traffic on a single network to only those nodes with the same NetBIOS scope ID.
WINS Server 1:	A Windows Internet Name Service (WINS) server IP to provide to connecting clients. Not desirable in most all modern networks.
WINS Server 2:	A Windows Internet Name Service (WINS) server IP to provide to connecting clients. Not desirable in most all modern networks.
Advanced:	Enter any additional options you would like to add to the OpenVPN server configuration here, separated by a semicolon. EXAMPLE: push "route 10.0.0.0 255.255.255.0"

Next

The wizard will now setup firewall rules. To proceed: click **Next**(shown below).

OpenVPN Remote Access Server Setup Wizard

Firewall Rule Configuration

Firewall rules control what network traffic is permitted. You must add rules to allow traffic to the OpenVPN server's IP and port, as well as allowing traffic from connected clients through the tunnel. These rules can be automatically added here, or configured manually after completing the wizard.

Traffic from clients to server

Firewall Rule: ☑ Add a rule to permit connections to this OpenVPN server process from clients anywhere on the Internet.

Traffic from clients through VPN

OpenVPN rule: ☑ Add a rule to allow all traffic from connected clients to pass inside the VPN tunnel.

Next

The wizard is now done configuring you VPN. To proceed: click **Next**(shown below).

OpenVPN Remote Access Server Setup Wizard

Configuration Complete!

Your configuration is now complete.

To be able to export client configurations, browse to System->Packages and install the OpenVPN Client Export package.

Finish

When finished you will see your server configuration as shown below.

Server | Client | Client Specific Overrides | Wizards | Client Export | Shared Key Export

Disabled	Protocol / Port	Tunnel Network	Description	
NO	UDP / 1194	10.10.10.0/24	JabVPN	

Additional OpenVPN servers can be added here.

2.9.3-OpenVPN Client Connectors

The client export connectors **MUST** be installed in order for any client to connect to your new VPN server. You should be able to use the ***default*** settings(pictured below) for your connector packages.

Server | Client | Client Specific Overrides | Wizards | Client Export | Shared Key Export

Remote Access Server	JabVPN UDP:1194
Host Name Resolution	Interface IP Address
Verify Server CN	Automatic - Use verify-x509-name (OpenVPN 2.3+) where possible Optionally verify the server certificate Common Name (CN) when the client connects. Current clients, including the most recent versions of Windows, Viscosity, Tunnelblick, OpenVPN on iOS and Android and so on should all work at the default automatic setting. Only use tls-remote if you must use an older client that you cannot control. The option has been deprecated by OpenVPN and will be removed in the next major version. With tls-remote the server CN may optionally be enclosed in quotes. This can help if the server CN contains spaces and certain clients cannot parse the server CN. Some clients have problems parsing the CN with quotes. Use only as needed.
Use Random Local Port	☑ Use a random local source port (lport) for traffic from the client. Without this set, two clients may not run concurrently. NOTE: Not supported on older clients. Automatically disabled for Yealink and Snom configurations.
Certificate Export Options	☐ Use Microsoft Certificate Storage instead of local files. ☐ Use a password to protect the pkcs12 file contents or key in Viscosity bundle.
Use Proxy	☐ Use proxy to communicate with the server.
Management Interface OpenVPNManager	☐ This will change the generated .ovpn configuration to allow for usage of the management interface. And include the OpenVPNManager program in the "Windows Installers". With this OpenVPN can be used also by non-administrator users. This is also useful for Windows Vista/7/8 systems where elevated permissions are needed to add routes to the system. NOTE: This is not currently compatible with the 64-bit OpenVPN installer. It will work with the 32-bit installer on a 64-bit system.
Additional configuration options	Enter any additional options you would like to add to the OpenVPN client export configuration here, separated by a line break or semicolon EXAMPLE: remote-random;

At the bottom of the page you will find **hyperlinks** for all the **Client Install Packages** in the **Exports** column on the right(shown below). Simply click the link for the package you wish to download.

Client Install Packages

User	Certificate Name	Export
Authentication Only (No Cert)	none	- Standard Configurations: Archive File Only - Inline Configurations: Android OpenVPN Connect (iOS/Android) Others - Windows Installers (2.3.8-Ix01): x86-xp x64-xp x86-win6 x64-win6 - Mac OS X: Viscosity Bundle

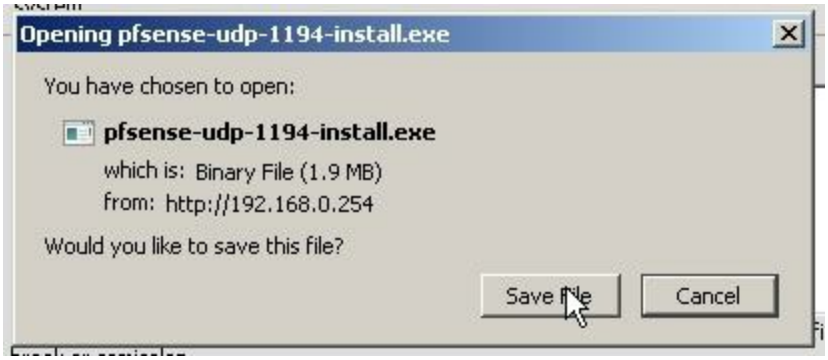
NOTES: The "XP" Windows installers work on Windows XP and later versions. The "win6" Windows installers include a new tap-windows6 driver that works only on Windows Vista and later.

If you expect to see a certain client in the list but it is not there, it is usually due to a CA mismatch between the OpenVPN server instance and the client certificates found in the User Manager.

Links to OpenVPN clients for various platforms:

OpenVPN Community Client - Binaries for Windows, Source for other platforms. Packaged above in the Windows Installers
OpenVPN For Android - Recommended client for Android
FEAT VPN For Android - For older versions of Android
OpenVPN Connect: Android (Google Play) or iOS (App Store) - Recommended client for iOS
Viscosity - Recommended client for Mac OS X
Tunnelblick - Free client for OS X

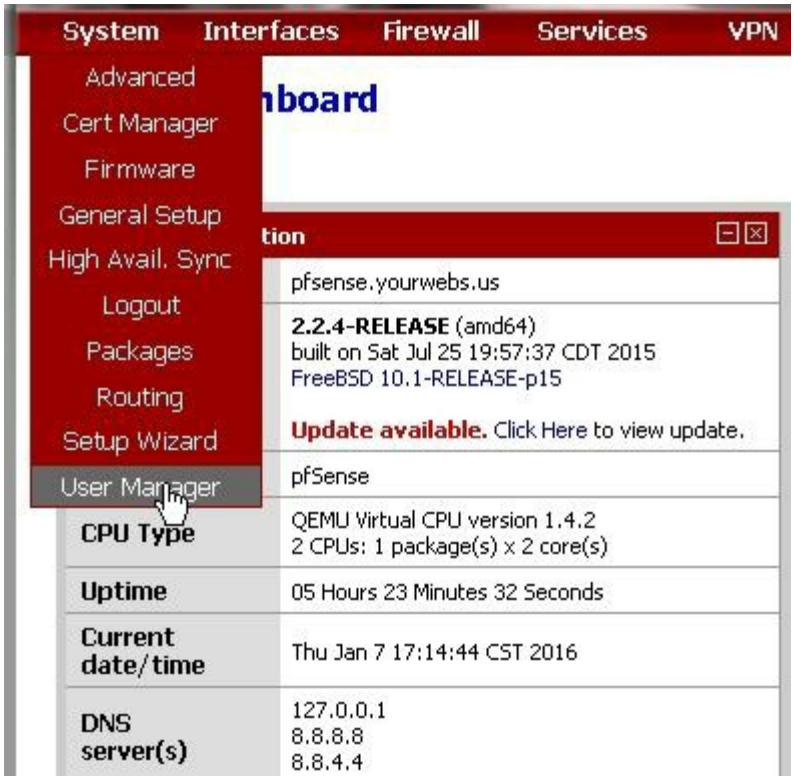
When the download dialog appears(pictured below) save the file to disk for installation on your client machines. **Please Note**: When ***installing*** connectors on ***Windows*** clients make sure to run the setup as ***Administrator***!



2.9.4-Authenticate Zentyal Domain Users

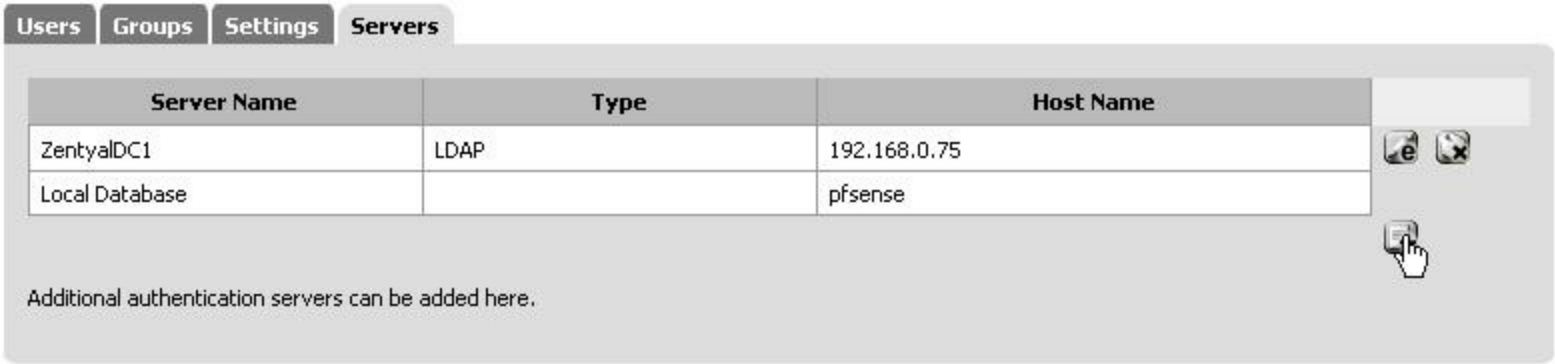
Now that we have a VPN server let's configure it so Domain users can authenticate and use it! To do this you first need to have Zentyal installed as covered in **Book 4: Zentyal Domain Controller**

With Zentyal installed let's proceed by clicking **System>User Manager**(shown below).



Next, click the **Servers** tab(shown below). Notice: the list below is already pre-populated with **ZentyalDC1** for your reference. Your installation should only show the **Local Database** at this point.

To add a new server click the + Button(shown below).



Next, you will need to enter your Zentyal Domain Controller information(shown below). **NOTICE**: The **Base DN** syntax must be entered ***exactly***. If your domain is **xyz.com** then the **Base DN** should be **DC=xyz,DC=com** or it will NOT work. This information can also be found in the ***Zentyal management interface*** under **Users and Computers>LDAP Settings.** Also, notice I have selected ***Microsoft AD*** as the **Initial Template**(pictured below). When finished click **Save**.

Users | Groups | Settings | Servers

Descriptive name ZentyalDC1

Type LDAP

LDAP Server Settings

Hostname or IP address 192.168.0.75
NOTE: When using SSL, this hostname MUST match the Common Name (CN) of the LDAP server's SSL Certificate.

Port value 389

Transport TCP - Standard

Peer Certificate Authority LRS-TEK
This option is used if 'SSL Encrypted' option is choosen.
It must match with the CA in the AD otherwise problems will arise.

Protocol version 3

Search scope
Level: One Level
Base DN: DC=yourwebs,DC=us

Authentication containers CN=Users,DC=yourwebs,DC=us Select
Containers: Note: Semi-Colon separated. This will be prepended to the search base dn above or you can specify full container path containing a dc= component.
Example: CN=Users;DC=example,DC=com
Example: OU=Staff;OU=Freelancers

Extended Query
Example: &(objectClass=inetOrgPerson)(mail=*@example.com)

Bind credentials
Use anonymous binds to resolve distinguished names
User DN: YOURWEBS\Administrator
Password: ●●●●●●●

Initial Template Microsoft AD

User naming attribute samAccountName

Group naming attribute cn

Group member attribute memberOf

UTF8 Encode
UTF8 encode LDAP parameters before sending them to the server. Required to support international characters, but may not be supported by every LDAP server.

Username Alterations
Do not strip away parts of the username after the @ symbol, e.g. user@host becomes user when unchecked.

Save

Now we'll test the new ***Authentication Server***. Select the server under the **Settings** tab the click **Save and Test**(shown below).

Users | Groups | Settings | Servers

Session Timeout

Time in minutes to expire idle management sessions. The default is 4 hours (240 minutes).
Enter 0 to never expire sessions. NOTE: This is a security risk!

Authentication Server: ZentyalDC1

Save | Save and Test

The test should run successfully as shown below. If not, re-check your settings and try again. When finished click **Close**(pictured below).

http://192.16...er=ZentyalDC1

192.168.0.254/system_usermanager_settings_test.php

pfSense

Testing pfSense LDAP settings... One moment please...

Attempting connection to	192.168.0.75	OK
Attempting bind to	192.168.0.75	OK
Attempting to fetch Organizational Units from	192.168.0.75	OK

Organization units found

CN=Users,DC=yourwebs,DC=us
OU=Domain Controllers,DC=yourwebs,DC=us

Close

To maintain the highest level of security we **only** want Zentyal Authenticating ***VPN Users***. Make sure to change **Authentication Server** back to **Local Database** after the test(shown below).

Users | Groups | Settings | Servers

Session Timeout

Time in minutes to expire idle management sessions. The default is 4 hours (240 minutes).
Enter 0 to never expire sessions. NOTE: This is a security risk!

Authentication Server: Local Database

Save | Save and Test

The final step is to ***enable*** the Zentyal server as a **Backend for authentication** in the **OpenVPN** server. To do this click **VPN>OpenVPN** then ***edit*** the server making sure the new **Zentyal** Server is **highlighted** as shown below. When finished don't forget to save the changes!

Server | Client | Client Specific Overrides | Wizards | Client Export | Shared Key Export

General information

Disabled	☐ **Disable this server** Set this option to disable this server without removing it from the list.
Server Mode	Remote Access (User Auth)
Backend for authentication	ZentyalDC1 Local Database
Protocol	UDP
Device Mode	tun
Interface	JAB
Local port	1194
Description	JabVPN You may enter a description here for your reference (not parsed).

2.10-Snort IDS

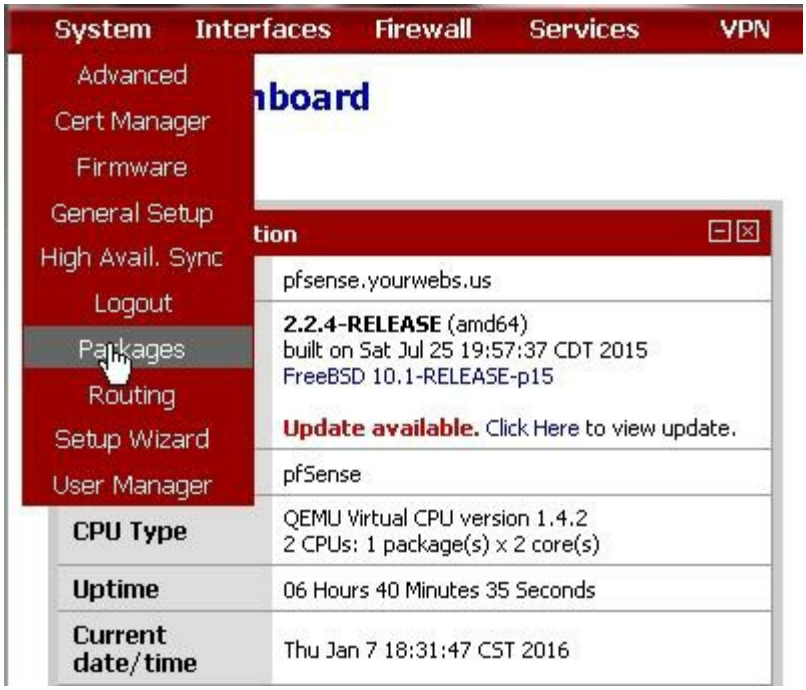
A critical component of any modern business network is intrusion detection or **IDS**. When it comes to IDS **Snort** is the most popular package used today! The concept behind IDS is to monitor transmission protocols for uncharacteristic behavior and then kill the connection when this behavior is detected. This is precisely the way Antivirus and Malware providers find new threats and create updates to counter those threats.

Most IDS systems are setup to monitor external connections by default. My recommendation is to monitor your internal connections instead. This method catches malicious code that can be brought in through portable devices such as smart-phones and USB thumb drives.

NOTE: Snort can be rather complicated to setup for those unfamiliar with it. This will be a quick run-through do to the many configuration options, so please make sure to duplicate my settings exactly! Let's get Snort working now!

2.10.1-Install Snort Package

To begin: click **System>Packages**(shown below).

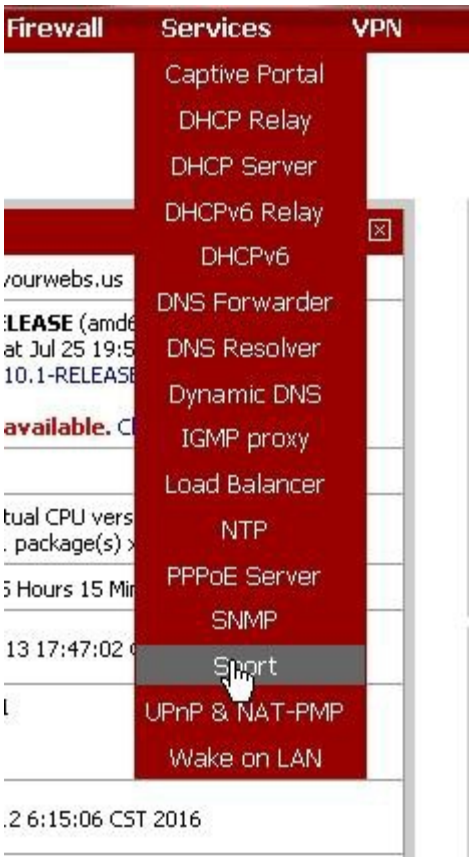


If you do not see ***Snort*** under **Installed Packages** download and install it under the **Available Packages** tab(pictured below).

Available Packages | Installed Packages

Name	Category	Version	Description
OpenVPN Client Export Utility	Security	Available: 1.3.0 Installed: 1.2.20	Allows a pre-configured OpenVPN Windows Client or Mac OS X's Viscosity configuration bundle to be exported directly from pfSense. No package info, check the forum
snort	Security	Available: 3.2.9.1 Installed: 3.2.8.2	Snort is an open source network intrusion prevention and detection system (IDS/IPS). Combining the benefits of signature, protocol, and anomaly-based inspection. Package info

Once the package is installed click **Services>Snort**(pictured below).



2.10.2-Snort Global Settings

Under the Global Settings tab(shown below) make sure **ONLY Emerging Threats** is checked. Duplicate all other settings.

Snort Interfaces | Global Settings | Updates | Alerts | Blocked | Pass Lists | Suppress | IP Lists | SID Mgmt | Log Mgmt | Sync

Please Choose The Type Of Rules You Wish To Download

Install **Snort VRT** rules	☐	Snort VRT free Registered User or paid Subscriber rules Sign Up for a free Registered User Rule Account Sign Up for paid Sourcefire VRT Certified Subscriber Rules
Install **Snort Community** rules	☐	The Snort Community Ruleset is a GPLv2 VRT certified ruleset that is distributed free of charge without any VRT License restrictions. This ruleset is updated daily and is a subset of the subscriber ruleset. **Note:** If you are a Snort VRT Paid Subscriber, the community ruleset is already built into your download of the Snort VRT rules, and there is no benefit in adding this rule set.
Install **Emerging Threats** rules	☑ ☐	ETOpen is an open source set of Snort rules whose coverage is more limited than ETPro. ETPro for Snort offers daily updates and extensive coverage of current malware threats. Sign Up for an ETPro Account **Note:** The ETPro rules contain all of the ETOpen rules, so the ETOpen rules are not required and are automatically disabled when the ETPro rules are selected.
Install **OpenAppID** detectors	☐	The OpenAppID package contains the application signatures required by the AppID preprocessor. **Note:** You must enable download of the OpenAppID detectors package in order to utilize the Application ID preprocessor and any user-provided application detection rules. Once enabled, go to the UPDATES tab and click to download updates.
Hide Deprecated Rules Categories	☐	Hide deprecated rules categories in the GUI and remove them from the configuration. Default is **Not Checked**.

Rules Update Settings

Update Interval	NEVER	Please select the interval for rule updates. Choosing **NEVER** disables auto-updates. **Hint:** in most cases, every 12 hours is a good choice.
Update Start Time	00:00	Enter the rule update start time in 24-hour format (HH:MM). **Default** is **00:05**. Rules will update at the interval chosen above starting at the time specified here. For example, using the default start time of 00:05 and choosing 12 Hours for the interval, the rules will update at 00:05 and 12:05 each day.

General Settings

Remove Blocked Hosts Interval	30 MINS	Please select the amount of time you would like hosts to be blocked. **Hint:** in most cases, 1 hour is a good choice.
Remove Blocked Hosts After Deinstall	☐	All blocked hosts added by Snort will be removed during package deinstallation.
Keep Snort Settings After Deinstall	☑	Settings will not be removed during package deinstallation.
Startup/Shutdown Logging	☐	Output detailed messages to the system log when Snort is starting and stopping. Default is **Not Checked**.

Save

Note: Changing any settings on this page will affect all Snort-configured interfaces.

2.10.3-Snort Interfaces

Under the **Snort Interfaces** tab add an interface by clicking the + button(shown below). Notice: I have included a pre-populated interface for reference.

Snort Interfaces | Global Settings | Updates | Alerts | Blocked | Pass Lists | Suppress | IP Lists | SID Mgmt | Log Mgmt | Sync

Interface	Snort	Performance	Block	Barnyard2	Description
LAN	ENABLED	AC-BNFA	ENABLED	DISABLED	LAN

Note:
This is the **Snort Menu** where you can see an overview of all your interface settings.
New settings will not take effect until interface restart.

Click on the icon to add an interface.
Click on the icon to edit an interface and settings.
Click on the icon to delete an interface and settings.

icons will show current snort and barnyard2 status.
Click on the status icons to **toggle** snort and barnyard2 status.

For this example we will add the **LAN** interface(shown below), which will catch alerts caused by infected USB thumb drives and smart-phones.

Snort Interfaces | Global Settings | Updates | Alerts | Blocked | Pass Lists | Suppress | IP Lists | SID Mgmt | Log Mgmt | Sync

LAN Settings | LAN Categories | LAN Rules | LAN Variables | LAN Preprocs | LAN Barnyard2 | LAN IP Rep | LAN Logs

General Settings

Enable	☑ Enable or Disable
Interface	LAN — Choose which interface this Snort instance applies to. Hint: In most cases, you'll want to use WAN here.
Description	LAN Enter a meaningful description here for your reference.

For Alert Settings duplicate my options for normal operation. **IMPORTANT**: during initial learning you will want to **UNCHECK Block Offenders**. This is only temporary until you have ***monitored normal traffic*** and added any false alerts to the **suppression list**.

Alert Settings

Send Alerts to System Logs	☐ Snort will send Alerts to the firewall's system logs.
Block Offenders	☑ Checking this option will automatically block hosts that generate a Snort alert.
Kill States	☑ Checking this option will kill firewall states for the blocked IP
Which IP to Block	src — Select which IP extracted from the packet you wish to block Hint: Choosing BOTH is suggested, and it is the default value.

For Detection Performance Settings duplicate my settings(shown below).

Detection Performance Settings

Search Method	AC-BNFA — Choose a fast pattern matcher algorithm. **Default** is **AC-BNFA**. LOWMEM and AC-BNFA are recommended for low end systems, AC-SPLIT: low memory, high performance, short-hand for search-method ac split-any-any, AC: high memory, best performance, -NQ: the -nq option specifies that matches should not be queued and evaluated as they are found, AC-STD: moderate memory, high performance, ACS: small memory, moderate performance, AC-BANDED: small memory,moderate performance, AC-SPARSEBANDS: small memory, high performance.
Split ANY-ANY	☐ Enable splitting of ANY-ANY port group. **Default** is **Not Checked**. This setting is a memory/performance trade-off. It reduces memory footprint by not putting the ANY-ANY port group into every port group, but instead splits these rules off into a single port group. But doing so may require two port group evaluations per packet - one for the specific port group and one for the ANY-ANY port group, thus potentially reducing performance.
Search Optimize	☑ Enable search optimization. **Default** is **Checked**. This setting optimizes fast pattern memory when used with search-methods AC or AC-SPLIT by dynamically determining the size of a state based on the total number of states. When used with AC-BNFA, some fail-state resolution will be attempted, potentially increasing performance.
Stream Inserts	☐ Do not evaluate stream inserted packets against the detection engine. **Default** is **Not Checked**. This is a potential performance improvement based on the idea the stream rebuilt packet will contain the payload in the inserted one, so the stream inserted packet does not need to be evaluated.
Checksum Check Disable	☐ Disable checksum checking within Snort to improve performance. Hint: Most of this is already done at the firewall/filter level, so it is usually safe to check this box.

Leave all whitelist settings at default(shown below).

Choose the networks Snort should inspect and whitelist

Home Net	default — View List Choose the Home Net you want this interface to use. Note: Default Home Net adds only local networks, WAN IPs, Gateways, VPNs and VIPs. Hint: Create an Alias to hold a list of friendly IPs that the firewall cannot see or to customize the default Home Net.
External Net	default — View List Choose the External Net you want this interface to use. Note: Default External Net is networks that are not Home Net. Most users should leave this setting at default. Hint: Create a Pass List and add an Alias to it, and then assign the Pass List here for custom External Net settings.
Pass List	default — View List Choose the Pass List you want this interface to use. Note: This option will only be used when block offenders is on. Hint: The default Pass List adds local networks, WAN IPs, Gateways, VPNs and VIPs. Create an Alias to customize.

The suppression filter(shown below) will be auto-generated after initial monitoring and adding of the first suppression entry.

Choose a suppression or filtering file if desired

Alert Suppression and Filtering	lansuppress_53d8285ee50b3 — View List Choose the suppression or filtering file you want this interface to use. Note: Default option disables suppression and filtering.

Now that you are finished setting up the **LAN** interface click **Save**(shown below).

Arguments here will be automatically inserted into the Snort configuration.

Advanced configuration pass-through

Save

Note: Click to save settings and exit e you attempt to start Snort.

2.10.4-Updating Threat Rules

Under the **Updates** tab(shown below) simply click the **Update** button in the middle of the page.

Snort Interfaces | Global Settings | Updates | Alerts | Blocked | Pass Lists | Suppress | IP Lists | SID Mgmt | Log Mgmt | Sync

INSTALLED RULE SET MD5 SIGNATURE

Rule Set Name/Publisher	MD5 Signature Hash	MD5 Signature Date
Snort VRT Rules	Not Enabled	Not Enabled
Snort GPLv2 Community Rules	Not Enabled	Not Enabled
Emerging Threats Open Rules	574e97f02e5bf7901dbb938986a66d98	Monday, 12-Oct-15 05:37:51 CDT
Snort OpenAppID Detectors	Not Enabled	Not Enabled

UPDATE YOUR RULE SET

Last Update: Oct-12 2015 05:37

Result: success

Update | Force

MANAGE RULE SET LOG

View Log

Log is empty.

The log file is limited to 1024K in size and automatically clears when the limit is exceeded.

NOTE: Snort.org and EmergingThreats.net will go down from time to time. Please be patient.

2.10.5-Threat Rule Categories

Threat rule **categories** are ***specific*** to the selected interface. Since we have configured the **LAN** interface for monitoring you must edit that specific interface by clicking the edit(**e**) button on the right under the **Snort Interfaces** tab. Next, click the LAN Categories tab and select **ONLY** the rules shown below. Selecting ***other*** rules will **FLOOD** you with ***unnecessary alerts*** and should only be experimented with after you become familiar with Snort.

Snort Interfaces | Global Settings | Updates | Alerts | Blocked | Pass Lists | Suppress | IP Lists | SID Mgmt | Log Mgmt | Sync

LAN Settings | LAN Categories | LAN Rules | LAN Variables | LAN Preprocs | LAN Barnyard2 | LAN IP Rep | LAN Logs

Automatic flowbit resolution

Resolve Flowbits ☑ If checked, Snort will auto-enable rules required for checked flowbits. The Default is **Checked.**

Snort will examine the enabled rules in your chosen rule categories for checked flowbits. Any rules that set these dependent flowbits will be automatically enabled and added to the list of files in the interface rules directory.

Auto Flowbit Rules [View] Click to view auto-enabled rules required to satisfy flowbit dependencies

Note: Auto-enabled rules generating unwanted alerts should have their GID:SID added to the Suppression List for the interface.

Snort VRT IPS Policy selection

Use IPS Policy ☐ If checked, Snort will use rules from one of three pre-defined IPS policies.

Note: You must enable download of the Snort VRT rules to enable and use this option. Selecting this option disables manual selection of Snort VRT categories in the list below, although Emerging Threats categories may still be selected if enabled on the Global Settings tab. These will be added to the pre-defined Snort IPS policy rules from the Snort VRT.

Select the rulesets Snort will load at startup

[Select All] [Unselect All] [Save] Click to save changes and auto-resolve flowbit rules (if option is selected above)

☑	emerging-malware.rules
☑	emerging-trojan.rules
☑	emerging-worm.rules

2.10.6-Add Alerts To Suppression List

Once snort is running you WILL start seeing alerts as seen in the list below. You can add ***low-risk*** alerts to the suppression list by clicking the plus(+) button in the **SID** column(shown below). **HINT**: Use common sense when building your suppression list!

Snort Interfaces | Global Settings | Updates | Alerts | Blocked | Pass Lists | Suppress | IP Lists | SID Mgmt | Log Mgmt | Sync

Alert Log View Settings

Instance to inspect: (LAN) LAN — Choose which instance alerts you want to inspect.

Save or Remove Logs: Download — All log files will be saved. Clear — Warning: all log files will be deleted.

Auto Refresh and Log View: Save — Refresh ☐ Default is ON. 250 — Enter number of log entries to view. Default is 250.

Alert Log View Filter

Alert Log Filter Options: Show Filter — Click to display advanced filtering options dialog

Last 250 Alert Entries (Most recent entries are listed first)

Date	Pri	Proto	Class	Source	SPort	Destination	DPort	SID	Description
01/13/16 06:22:33	3	TCP	Unknown Traffic	152.163.13.67	80	192.168.0.41	53528	120:11	(http_inspect) MULTIPLE ENCODINGS WITHIN JAVASCRIPT OBFUSCATED DATA
01/09/16 01:28:22	3	TCP	Unknown Traffic	152.163.13.67	80	192.168.0.41	50437	120:11	(http_inspect) MULTIPLE ENCODINGS WITHIN JAVASCRIPT OBFUSCATED DATA

Once you have suppressed ***any*** alert the suppression list should be ***auto-generated*** as shown below.

Snort Interfaces | Global Settings | Updates | Alerts | Blocked | Pass Lists | Suppress | IP Lists | SID Mgmt | Log Mgmt | Sync

File Name	Description
lansuppress_53d8285ee50b3	Auto-generated list for Alert suppression

2.10.7-Block Offenders At Source

Once you have monitored your normal network traffic and established a suppression list it's time to ***let Snort work***. You can now go back to the **Snort Interface** settings and enable ***offenders to be blocked at the source***. Remember, this is the option I recommended you leave unchecked until you had a chance to monitor traffic.

IMPORTANT: Snort is very powerful and it **WILL** block traffic! It may even block You! If this happens login to pfSense from another computer, ***temporarily disable blocking***, and ***make sure*** to run a ***virus or malware*** scan on the blocked machine just to be safe! When setup and used properly this system **ROCKS**!

Snort Interfaces | Global Settings | Updates | Alerts | **Blocked** | Pass Lists | Suppress | IP Lists | SID Mgmt | Log Mgmt | Sync

Blocked Hosts Log View Settings

Save or Remove Hosts [Download] All blocked hosts will be saved. [Clear] **Warning:** all hosts will be removed.

Auto Refresh and Log View [Save] Refresh ☑ **Default** is **ON**. 500 Enter number of blocked entries to view. **Default** is **500**.

Last 500 Hosts Blocked by Snort

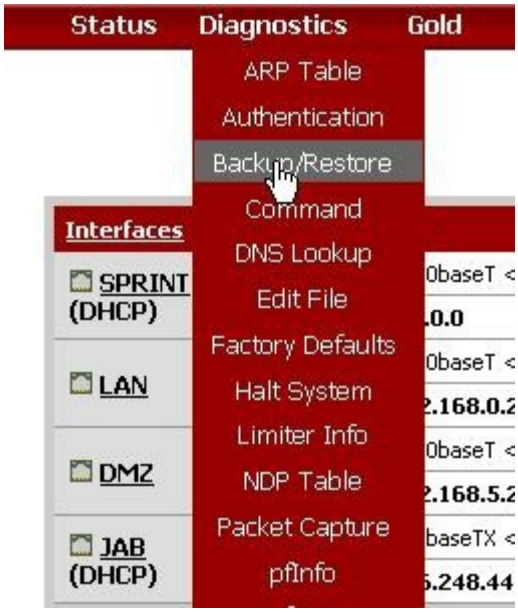
#	IP	Alert Description	Remove

There are currently no hosts being blocked by Snort.

2.11-Configuration Backups

Besides using VM image backups it is also wise to keep a copy of the pfSense configuration. The configuration backup is especially important when developers rewrite the build in a way that breaks certain packages on update. In these instances your VM image backup will only get you back to the version you were using. I have had this happen only 1 time in the last 7 years, so don't worry too much!

To access the configuration backup page: click **Diagnostics>Backup/Restore**(pictured below).



You should see the Backup/Restore dialog as shown below. Now, click the **Download configuration** button.

Config History | Backup/Restore

Backup configuration

Click this button to download the system configuration in XML format.

Backup area: ALL

☐ Do not backup package information.

☐ Encrypt this configuration file.

☑ Do not backup RRD data (NOTE: RRD Data can consume 4+ megabytes of config.xml space!)

Download configuration

Restore configuration

Open a configuration XML file and click the button below to restore the configuration.

Restore area: ALL

Browse... No file selected.

☐ Configuration file is encrypted.

Restore configuration

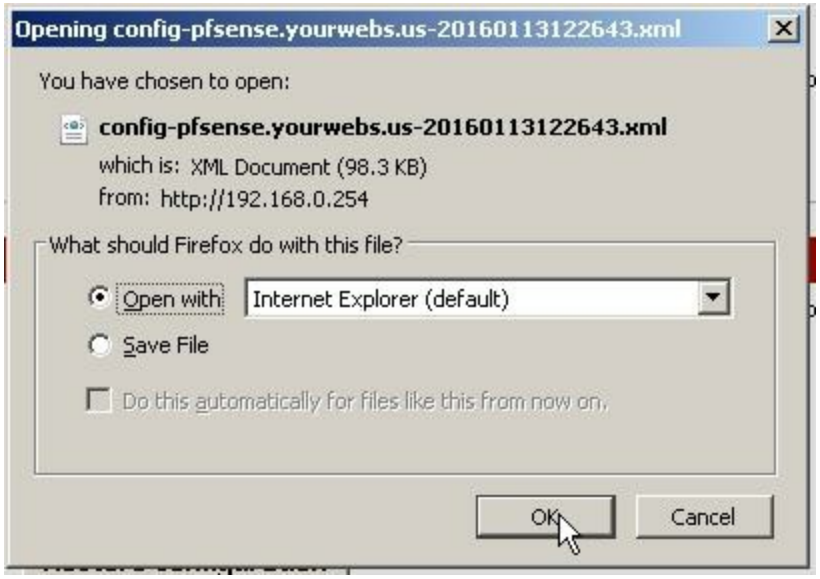
Note:
The firewall will reboot after restoring the configuration.

Package Functions

Click this button to reinstall all system packages. This may take a while.

Reinstall packages

When the download dialog appears(shown below) save your configuration to disk. HINT: I like to keep a copy of this on thumb drive!



Restoring your pfSense should be self-explanatory! Simply use the Restore configuration option instead!

Book 3: freeNAS

3.1-Traditional Storage Fails

For years I relied on traditional storage servers usually configured with either **RAID(1, 5, 6, or 10)**. My preferred file system was **XFS** because it was cutting edge and relatively trouble free. The problem was that a file server consumes the entire hardware resource of that machine even when there is no demand. Furthermore, you need multiple machines dedicated to storage in order to maintain data redundancy.

Another observation was that **RAID is NOT perfect**! If you select hardware RAID and the controller dies have fun getting the system back up in a timely manner! If you select software RAID and the file system degrades you'll take a huge performance hit while it rebuilds.

Large arrays can easily take 24hrs to complete this process. During this time the IT Department gets flooded with calls about poor system performance! To make matters worse, the automatic backup starts running it's nightly incremental causing performance to plummet! There had to be a better way!

What Makes A Good Storage System

How do you define a good storage system? First, I asked myself what was MOST important? Well, that's not easy to answer after being in the field and experiencing problems! There are several key elements involved!

For me, they are:

- The data storage platform MUST be ***reliable*** and ***compatible*** for years
- ***Complete*** system disaster ***recovery*** MUST be ***simple*** and ***fast***
- The storage ***input/output*** MUST be ***fast***
- ***Daily*** end-users ***restore*** requests must be ***simple*** and ***fast***
- Data MUST be ***redundantly*** stored
- Data ***corruption*** MUST be minimized

If I cannot meet **ALL** of these expectations then the storage platform choice is wrong! According to these needs traditional **RAID(1, 5, 6, or 10)** storage simply could not work! This requires an explanation!

Duty Cycles

When engineers design electronic components they commonly provide a Duty Cycle Rating. This special rating helps determine how long a component can perform under load before heat buildup starts irreversibly degrading components. Now, let's apply this concept to a hard disk array!

When a parity array such as **RAID(1, 5, 6, or 10)** is written to it must synchronize the data cache without interruption or it WILL degrade. If it degrades, it WILL rebuild! If it rebuilds, it introduces extended duty cycle and heat buildup. This heat buildup irreversibly degrades components leading to eventual failure.

A striping array such as **RAID-0** never synchronizes or degrades. This reduces duty cycle and heat buildup thus increasing component life. It also provides increased throughput as a bonus!

Simplicity & Redundancy

RAID-0(striping array) fits the performance demand perfectly. It can NEVER degrade! It either works or it doesn't! What about simplicity and redundancy?

So here's the magic! We build our system using **ONLY** non-parity striping arrays then use **RSync to replicate** the data over **several NAS machines**. This gives the performance of **RAID-0** while maintaining data redundancy.

This method provides data input/output rates that beat **ANY** RAID-10 storage. Furthermore, when virtualized, **ALL** platform **compatibility** issues for on the fly upgrades are gone. Best of all, Linux LVM provides a simple method of creating ***UUID serialized stripe volumes***. This means bullet-proof booting and easy physical migrations to other machines.

It seems that all the requirements are satisfied except ***end-user restore requests*** and ***minimizing data corruption***. Waite, there's **freeNAS** with **ZFS**!

3.2-freeNAS & ZFS

The final requirements are satisfied with the addition of the self-healing **ZFS** file system. The best purpose built distribution for this is **freeNAS**. When setup according to this book you can expect very respectable performance when compared to bare metal file servers. **freeNAS** is very complete with active directory integration, snapshot backups, and a super built-in RSync script for hands free duplication across nodes. Let's get on with the installation!

NOTE: freeNAS is a powerful platform and it's feature-set cannot be completely covered in this book. This guide was designed as a step-by-step to get you up and running quickly. I highly recommend tapping the wealth of online resources available for a more thorough understanding.

3.3-Installing freeNAS

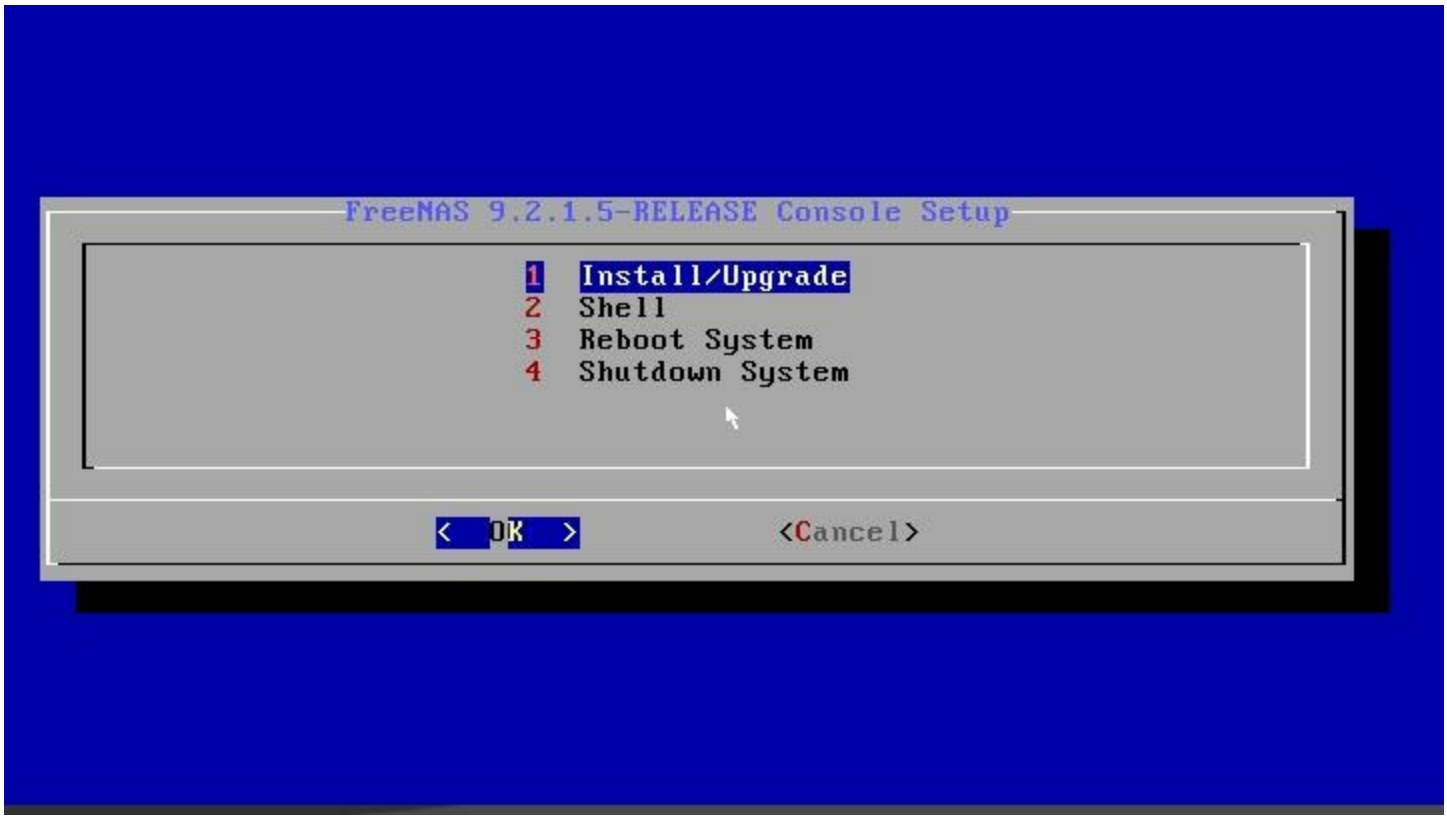
Before installation can begin you must ***create the VM configuration***. I recommend a ***8Gb IDE virtual disk*** with ***8Gb of Ram*** for this install. If you need to review those steps again click here: **1.9-Creating VM Configuration**

Now, power on the freeNAS VM making sure that you have the CD or disk image loaded. For this book I have used freeNAS version 9.2.1.5-RELEASE -x64.iso. If you do not have freeNAS you can download the latest release here: http://www.freenas.org/download-freenas-release.html

NOTE: The download section also allows you to choose other releases toward the bottom of the page. I would recommend using the exact version I have used for this book! It has proven **VERY** reliable and if it's **NOT BROKEN** don't try to fix it!

Once powered up you should see the following screens:

To proceed: press **ENTER** (indicating **OK**)

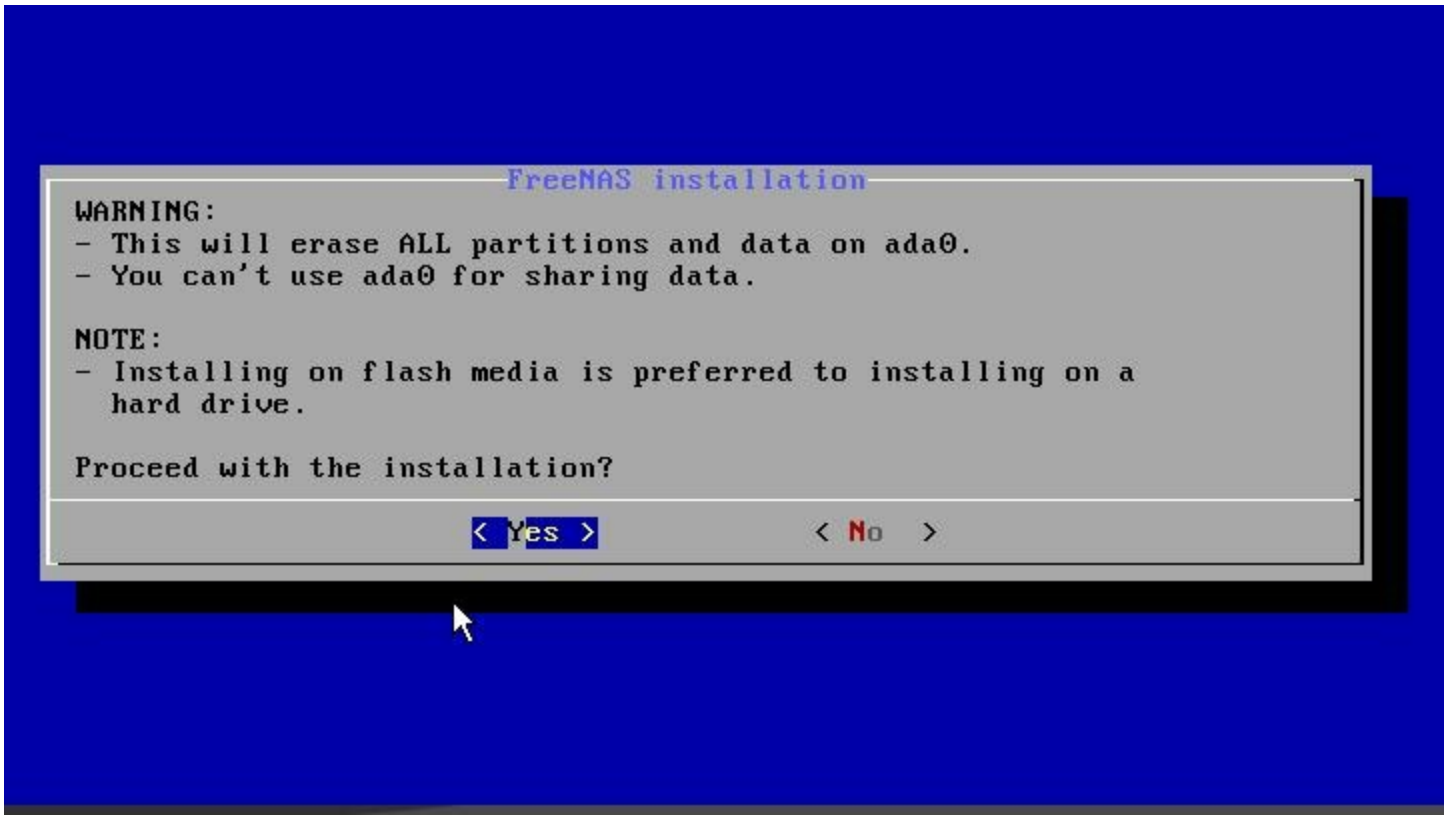


Next, you will be prompted for the installation hard disk(pictured below). Since we only have one disk this is easy!

To proceed: press **ENTER** (indicating **OK**)

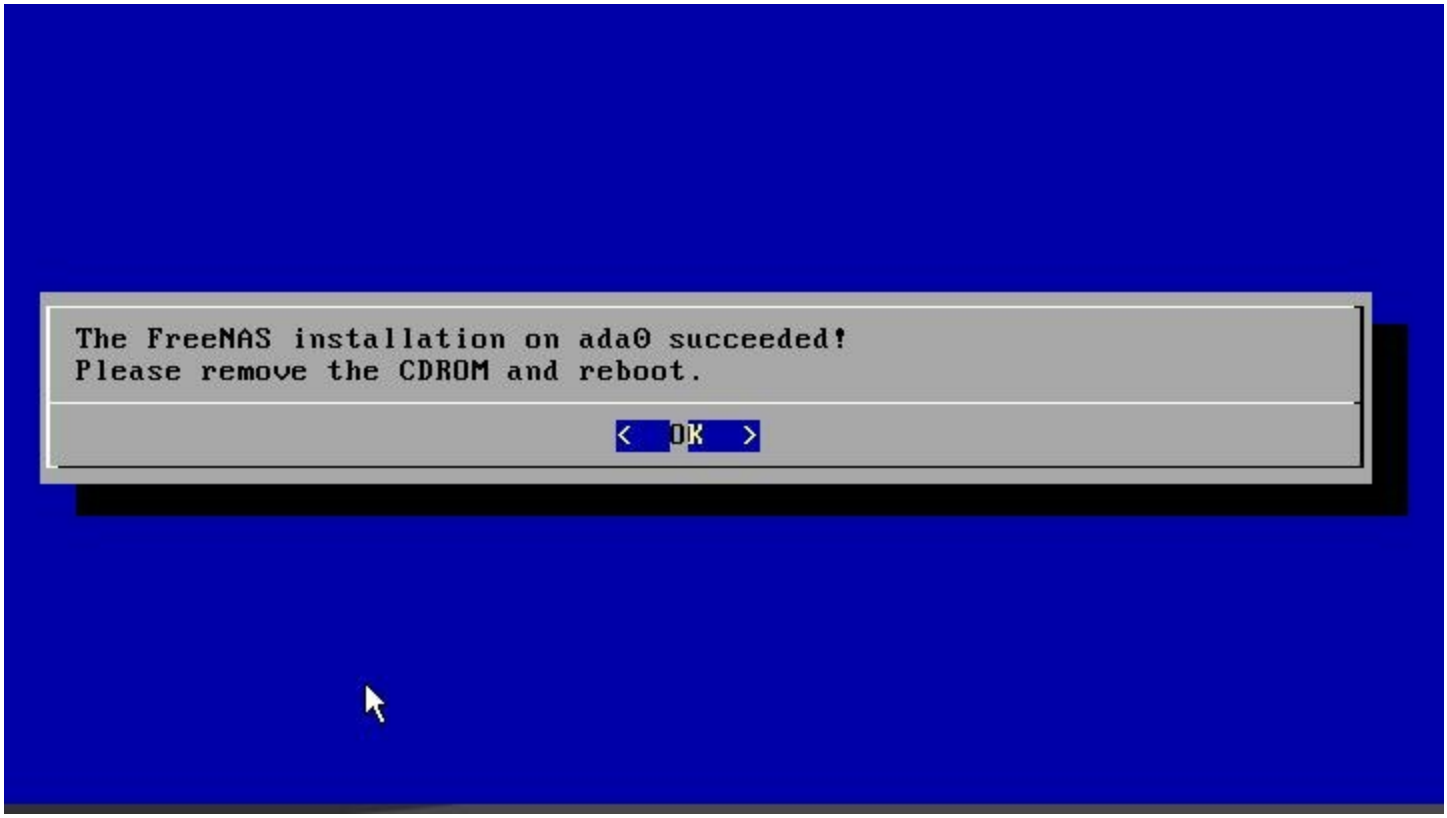
freeNAS is now ready to begin the install(pictured below).

To proceed: press **ENTER** (indicating **Yes**)



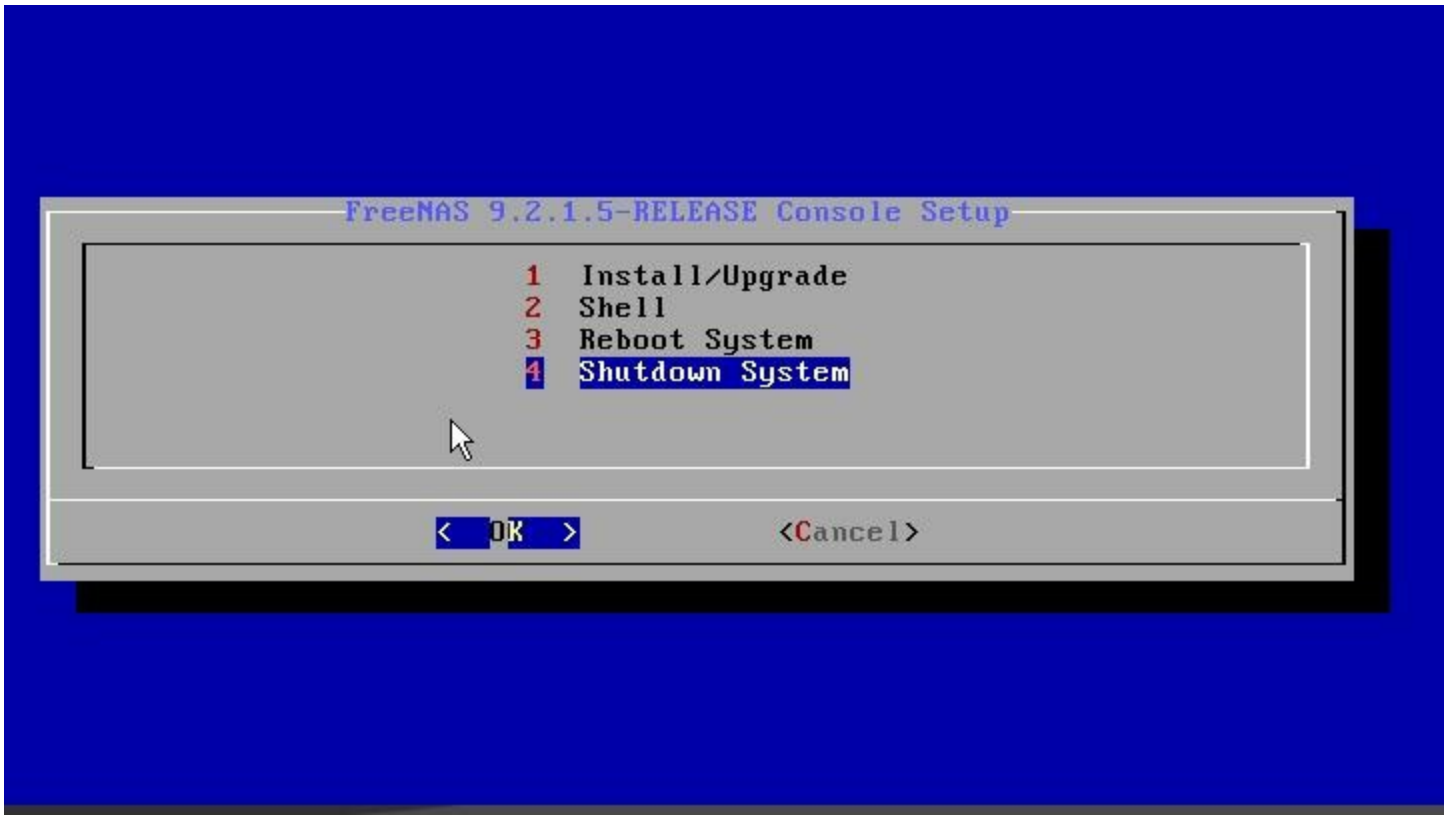
When the install is completed you will be prompted to remove the CD and reboot(pictured below).

To proceed: press **ENTER** (indicating **OK**)

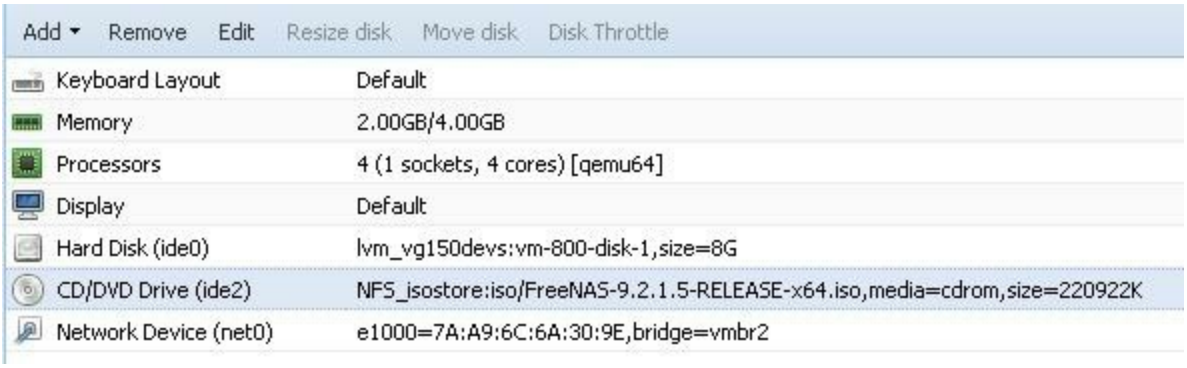


In order to remove the CD you will need to select list item 4-shutdown(pictured below).

To proceed: press **ENTER** (indicating **OK**)

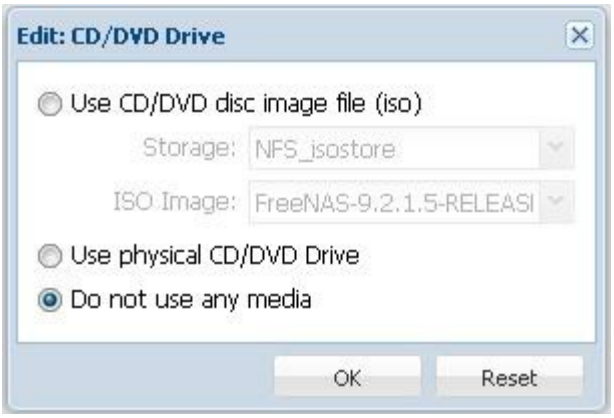


Now you can close the console and go to the VM hardware tab(pictured below). Select the CD then click **Edit**

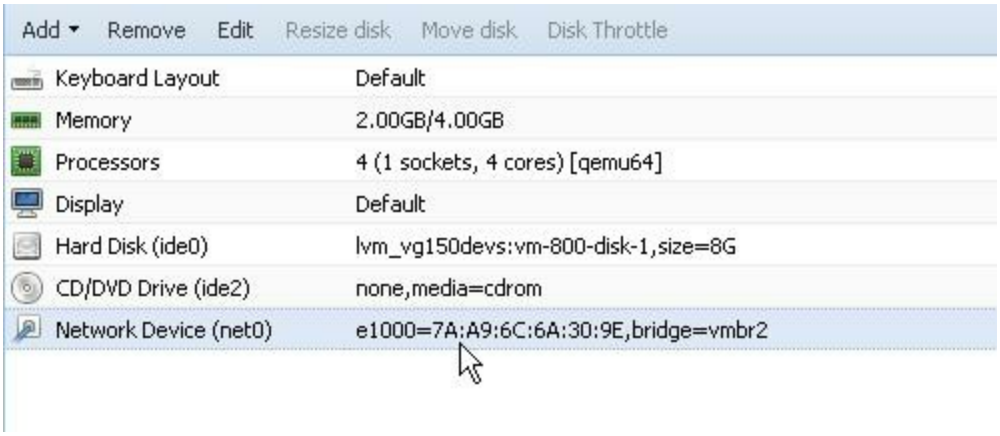


To prevent the freeNAS VM from using the CD drive again simply check **Do not use any media**(pictured below).

To proceed: click **OK**



Next, you need to copy the network interface Mac\hardware address(highlighted below) so that it can be entered into the pfSense router, which should already be installed.



Now, open your pfSense web management interface and make the appropriate entry in the DHCP static mappings(pictured below). Don't forget to save your changes.

System Interfaces Firewall Services VPN Status Diagnostics Gold Help

Services: DHCP: Edit static mapping

Static DHCP Mapping on LAN

MAC address	7a:a9:6c:6a:30:9e Copy my MAC address Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx
Client identifier	
IP address	192.168.0.22 If an IPv4 address is entered, the address must be outside of the pool. If no IPv4 address is given, one will be dynamically allocated from the pool.
Hostname	freeNAS-4 Name of the host, without domain part.
Description	You may enter a description here for your reference (not parsed).
ARP Table Static Entry	☑ Create an ARP Table Static Entry for this MAC & IP Address pair.

3.4-Add freeNAS Pass-Through Disks

At this point there is no storage drive for freeNAS to use for shares. We will now add the ***LVM striped volume*** that was created in **Chapter 1.12** as a **pass-through** hard disk. You may wish to revisit that chapter!

To begin, open the PuTTY program and login as ***root*** on your Proxmox server(pictured below).

```
login as: root
root@192.168.0.16's password:
Linux proxmox3 2.6.32-32-pve #1 SMP Thu Aug 21 08:50:19 CEST 2014 x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Fri Nov 27 05:47:56 2015 from win7pro.yourwebs.us
root@proxmox3:~# qm set 800 -ide1 /dev/freenas4/6tbstore
```

To assign the new disk we will issue the special QEMU command as follows:

qm set 800 -ide1 /dev/freenas4/6tbstore

The command entered into PuTTY looks like this(pictured below).

```
login as: root
root@192.168.0.16's password:
Linux proxmox3 2.6.32-32-pve #1 SMP Thu Aug 21 08:50:19 CEST 2014 x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Fri Nov 27 05:47:56 2015 from win7pro.yourwebs.us
root@proxmox3:~# qm set 800 -ide1 /dev/freenas4/6tbstore
update VM 800: -ide1 /dev/freenas4/6tbstore
root@proxmox3:~#
```

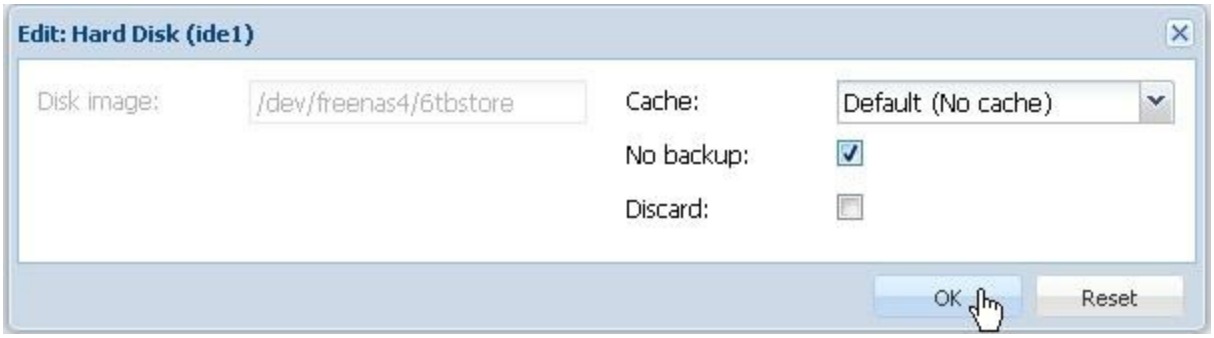
The result of this command is evident by the new IDE1 drive shown in the freeNAS-4 hardware window(pictured below). **NOTE**: You will need to refresh the tab page before the new disk will appear.

Add ▾ Remove Edit Resize disk Move disk Disk Throttle

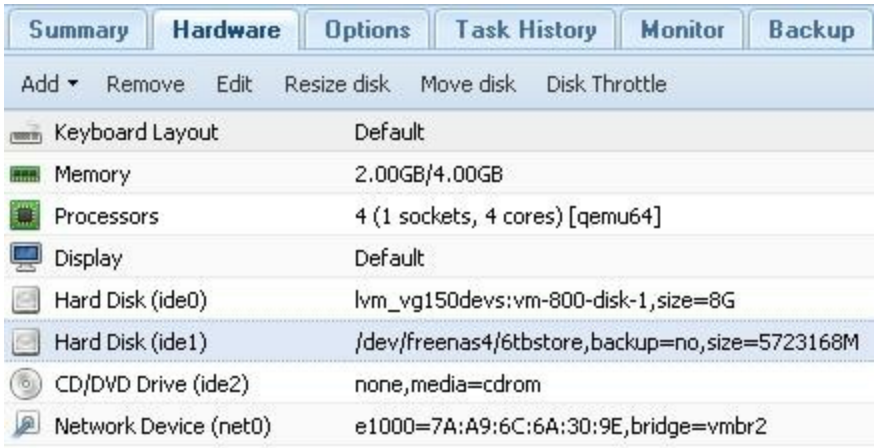
Keyboard Layout	Default
Memory	2.00GB/4.00GB
Processors	4 (1 sockets, 4 cores) [qemu64]
Display	Default
Hard Disk (ide0)	lvm_vg150devs:vm-800-disk-1,size=8G
Hard Disk (ide1)	/dev/freenas4/6tbstore,size=5723168M
CD/DVD Drive (ide2)	none,media=cdrom
Network Device (net0)	e1000=7A:A9:6C:6A:30:9E,bridge=vmbr2

3.5-Set Storage For No Backup

IMPORTANT: It is extremely important that we **ONLY** backup the freeNAS primary disk(**ide0**) and **NOT** the 6TB storage drive. If this were to happen it would seriously degrade your system performance! Your backups should be configured using **RSync** from ***within*** the freeNAS **guest**. This behavior can easily be avoided by editing the disk properties as shown below.



Notice the disk properties(pictured below) indicate that secondary disk(**ide1**) will **NOT** be included in backups.

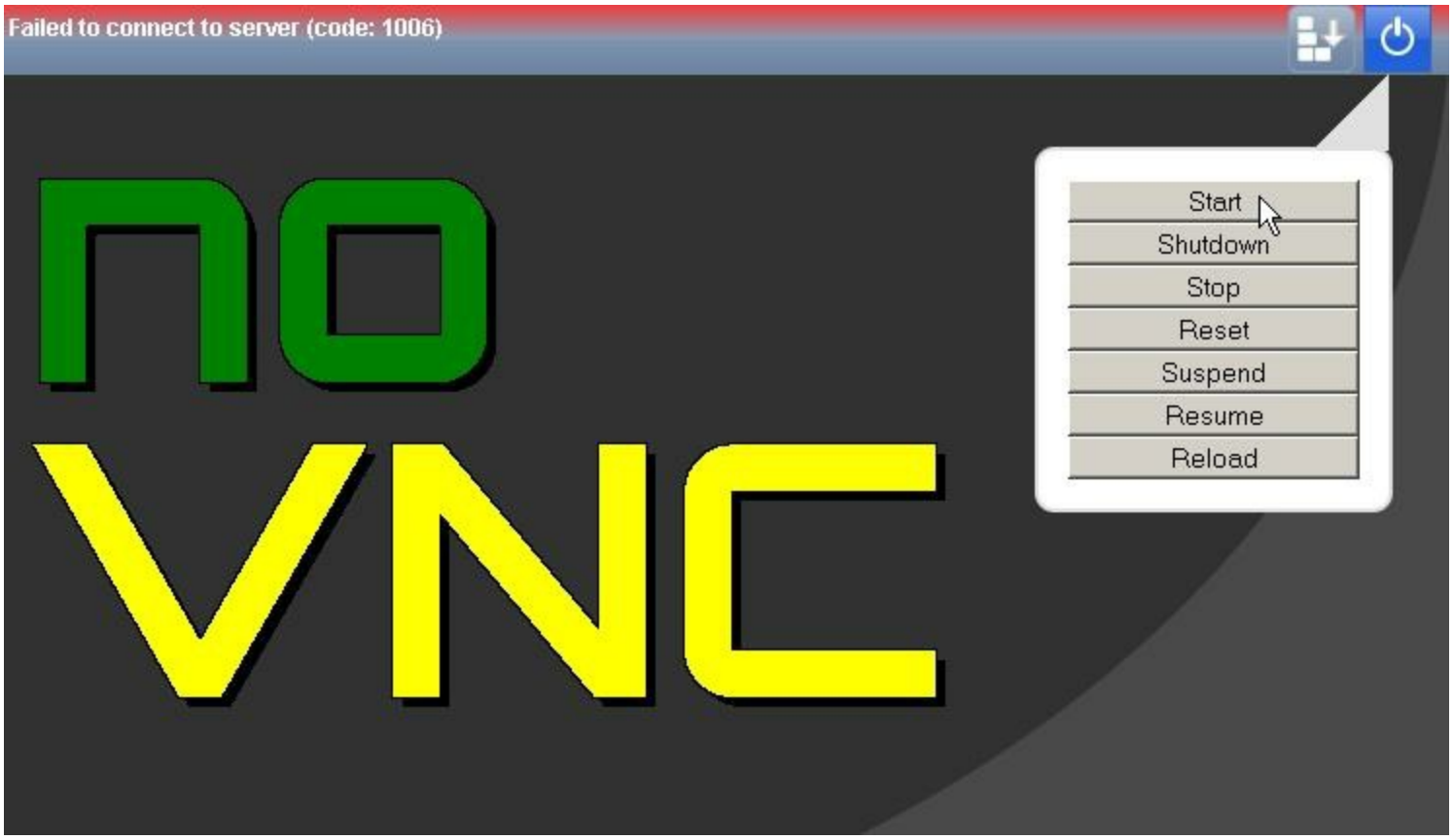


The freeNAS-4 VM(above) can now be booted and the new 6TB disk configured as a ZFS stripe.

PLEASE REMEMBER: It is important to note that freeNAS-4 is now tied to the Proxmox3 server by its hardware pass-through disk. It cannot be moved to another physical machine unless the physical disks are removed.

3.6-Start freeNAS Through The Console

Now, start your new freeNAS VM by opening the Proxmox console in the upper right hand corner. When the console appears click the **Start** Button(pictured below).



We are only using the console window startup to ensure the VM starts properly and is assigned the appropriate IP address through DHCP. Notice the bottom of the console display indicates our web interface address to be **http://192.168.0.22**

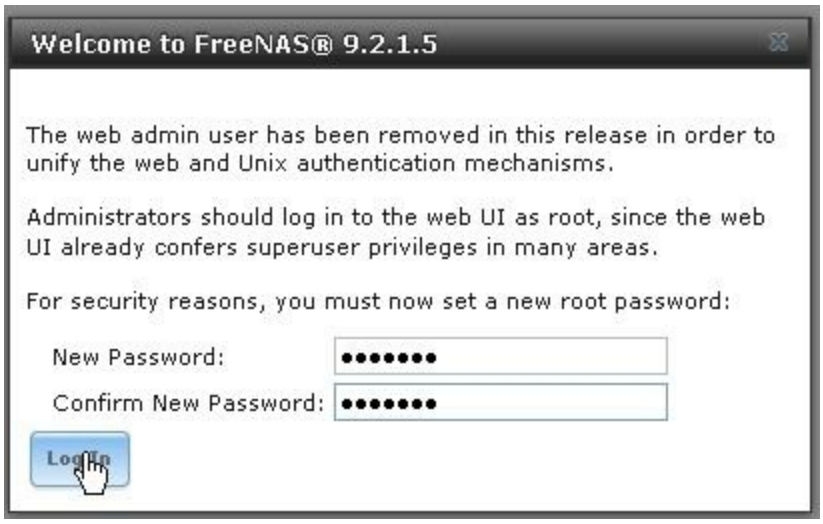
Connected (encrypted) to: QEMU (freeNAS-4)

```
Fri Dec 11 14:03:47 PST 2015

FreeBSD/amd64 (freenas.local) (ttyv0)


Console setup
-------------

1) Configure Network Interfaces
2) Configure Link Aggregation
3) Configure VLAN Interface
4) Configure Default Route
5) Configure Static Routes
6) Configure DNS
7) Reset WebGUI login credentials
8) Reset to factory defaults
9) Shell
10) Reboot
11) Shutdown

You may try the following URLs to access the web user interface:

http://192.168.0.22
```

3.7-Initial Login

Now, you can open the web browser and enter the address of the freeNAS VM. I use and recommend Mozilla Firefox.

The first screen you see will be the ***root user*** password change dialog(shown below). Make your password strong!



Once the password is set you should see the full web management interface(pictured below).

FreeNAS®

System Network Storage Sharing Services Plugins Jails Reporting Account Help Log Out Alert

expand all collapse all

- Account
- System
- Network
- Storage
- Sharing
- Services
- Plugins
- Jails
- Reporting
- Display System Processes
- Shell
- Reboot
- Shutdown

Settings X System Information X

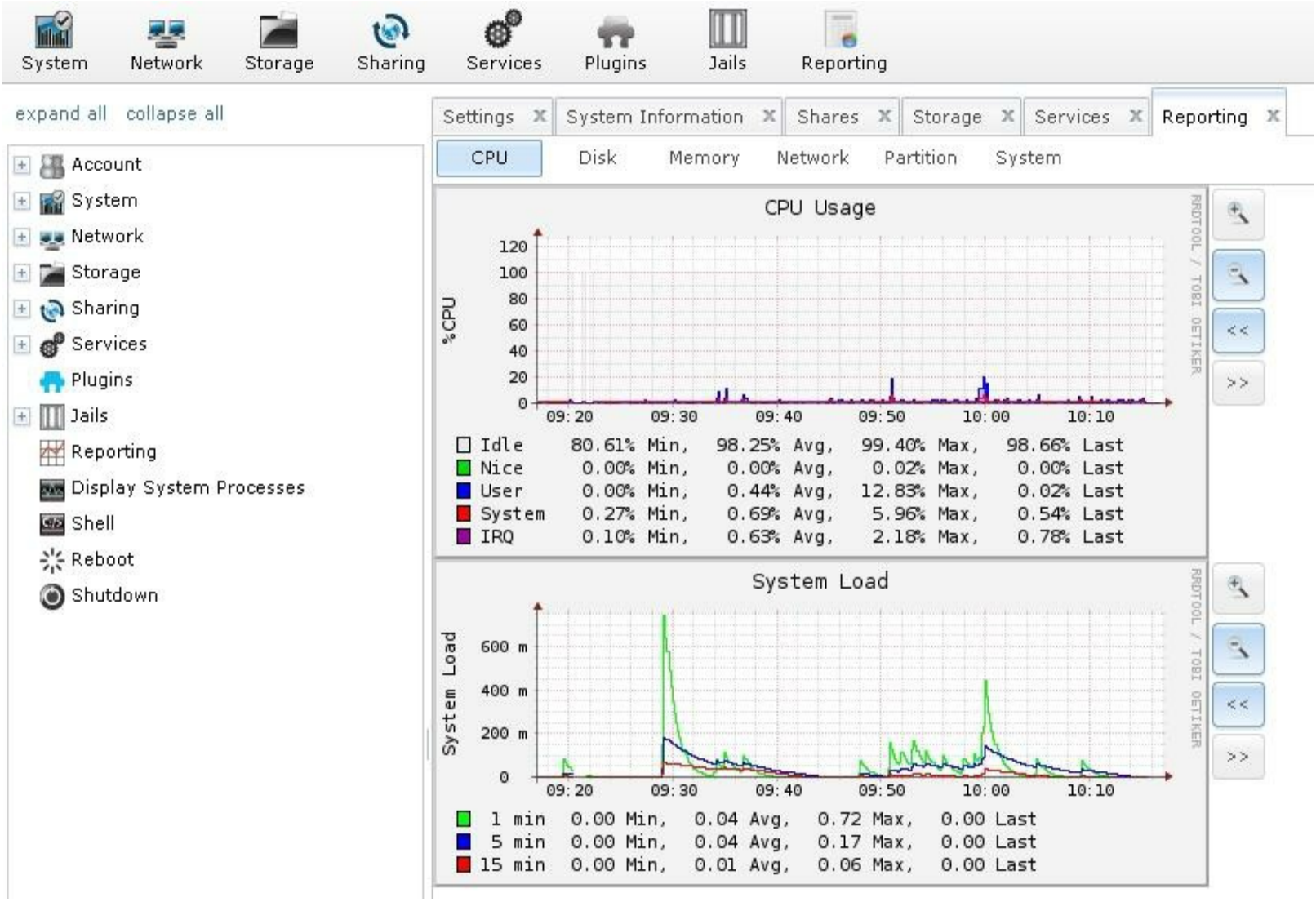
System Information

Hostname	freenas.local Edit
Build	FreeNAS-9.2.1.5-RELEASE-x64 (80c1d35)
Platform	QEMU Virtual CPU version 2.1.0
Memory	4075MB
System Time	Fri Dec 11 14:07:35 PST 2015
Uptime	2:07PM up 5 mins, 0 users
Load Average	0.10, 0.22, 0.14

FreeNAS® © 2014 iXsystems, Inc.

3.8-freeNAS Navigation

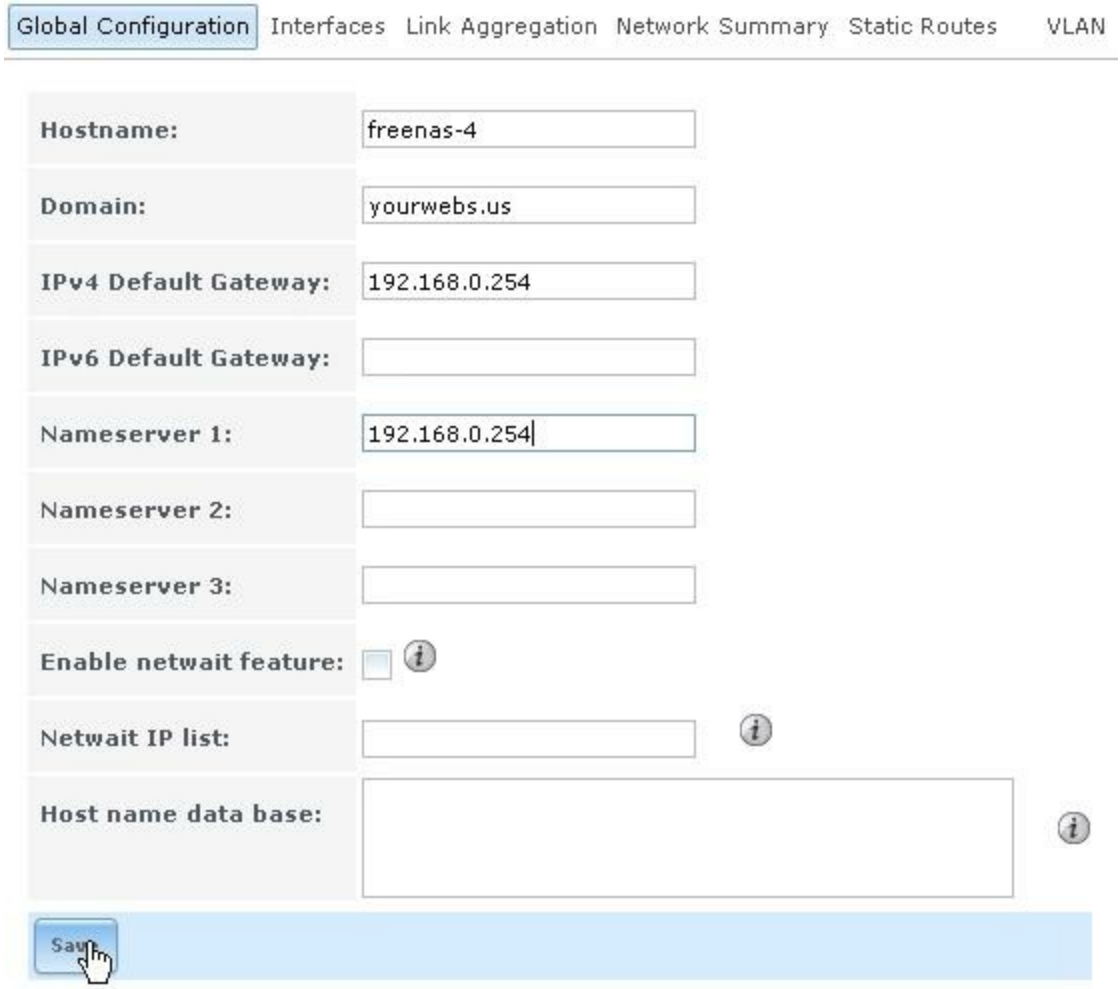
Navigation is pretty straight forward! You will find a series of tabs at the top of the main screen. There is also a tree in the left column(pictured below).



3.9-Network Configuration

During installation freeNAS defaults to accept **DHCP** with its hostname set to **freenas**. **DHCP** is **NOT** desired when you run servers of any kind. Furthermore, with multiple freenas machines running on your network they cannot all have the same name! Let's change that now!

Under the **Network>Global Configuration** tab(pictured below) you can change your Hostname, Domain, Gateway, and Nameserver information. In this case I have set the Gateway and Nameserver to the IP address of the pfSense Router running on Proxmox. Don't forget to save your changes!



Now, let's click on the **Network Summary** (shown below) tab to verify our network interface name and address. This will be needed to setup a static address mapping.

Next, click **Interfaces>Add Interface**(pictured below).

When the interface dialog appears(shown below) enter the appropriate **Interface Name** and **IP Address**. The **Netmask** will almost **ALWAYS** be (**255.255.255.0**). This is the most commonly used **Netmask** for home or business reservation ranges.

Add Interface

NIC: em0

Interface Name: em0

DHCP:

IPv4 Address: 192.168.0.22

IPv4 Netmask: /24 (255.255.255.0)

Auto configure IPv6:

IPv6 Address:

IPv6 Prefix Length: ---------

Options:

Alias

IPv4 Address:

IPv4 Netmask: ---------

IPv6 Address:

IPv6 Prefix Length: ---------

Add extra Alias

OK Cancel

When finished you should see the new entry listed under Interfaces(shown below).

Global Configuration | Interfaces | Link Aggregation | Network Summary | Static Routes | VLAN

Add Interface

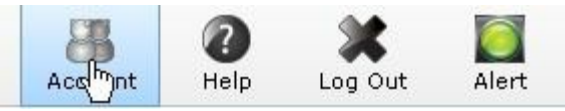
NIC	Interface Name	DHCP
em0	em0	false

3.10-Users And Groups

3.10.1-Adding A New User

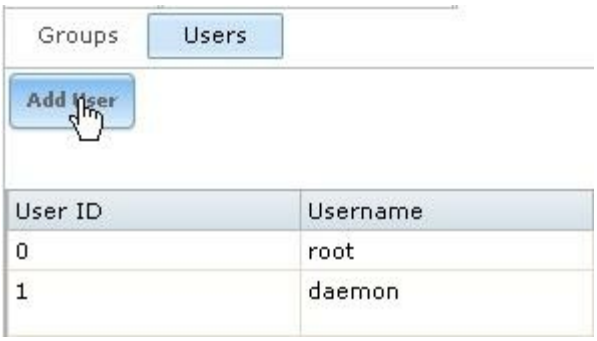
If you do not have a domain running locally you will need to add users to your server or servers. At the far right of the main interface you will find the **Account button**(pictured below).

To proceed: click **Account**



You should then see the default **Users** and **Groups** page. You can easily navigate using the tabs at the top of the page.

To add a member: click **Add User**(shown below)



The **Add User** dialog should then appear(shown below). Enter the new User information as required. I have included sample data for reference.

Add User

User ID:	1001
Username:	jsmith
Create a new primary group for the user:	☑
Primary Group:	-----
Home Directory:	/nonexistent Browse
Home Directory Mode:	Owner Group Other Read ☑ ☑ ☑ Write ☑ ☐ ☐ Execute ☑ ☑ ☑
Shell:	csh
Full Name:	John Smith
E-mail:	jsmith@yourwebs.us
Password:	•••••••
Password confirmation:	•••••••
Disable password login:	☐
Lock user:	☐
Permit Sudo:	☐
SSH Public Key:	

At the bottom of the entry form there is a section allowing you to choose **Auxiliary groups** for the new user. Let's add John Smith to the ftp group! To do so simply double click the appropriate group from the **Available** column(pictured below).

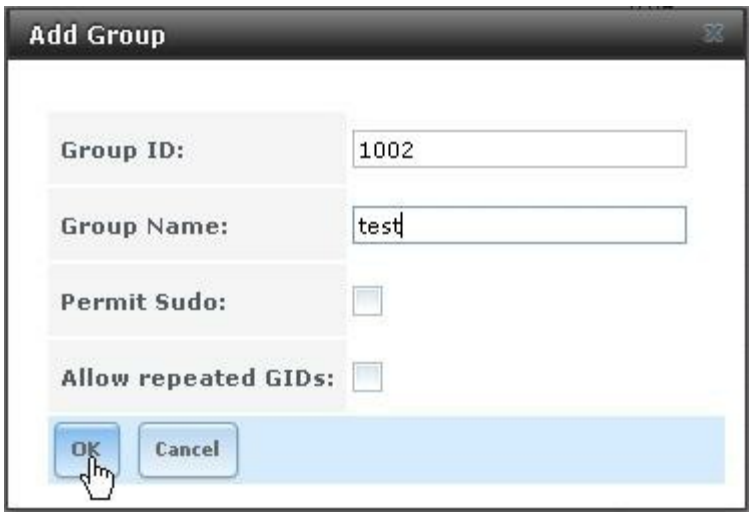
	Available		Selected
Auxiliary groups:	wheel daemon kmem sys	<<	ftp
		>>	

3.10.2-Adding A New Group

To add a new group is equally simple.

To add a member: click **Add Group**(shown below)

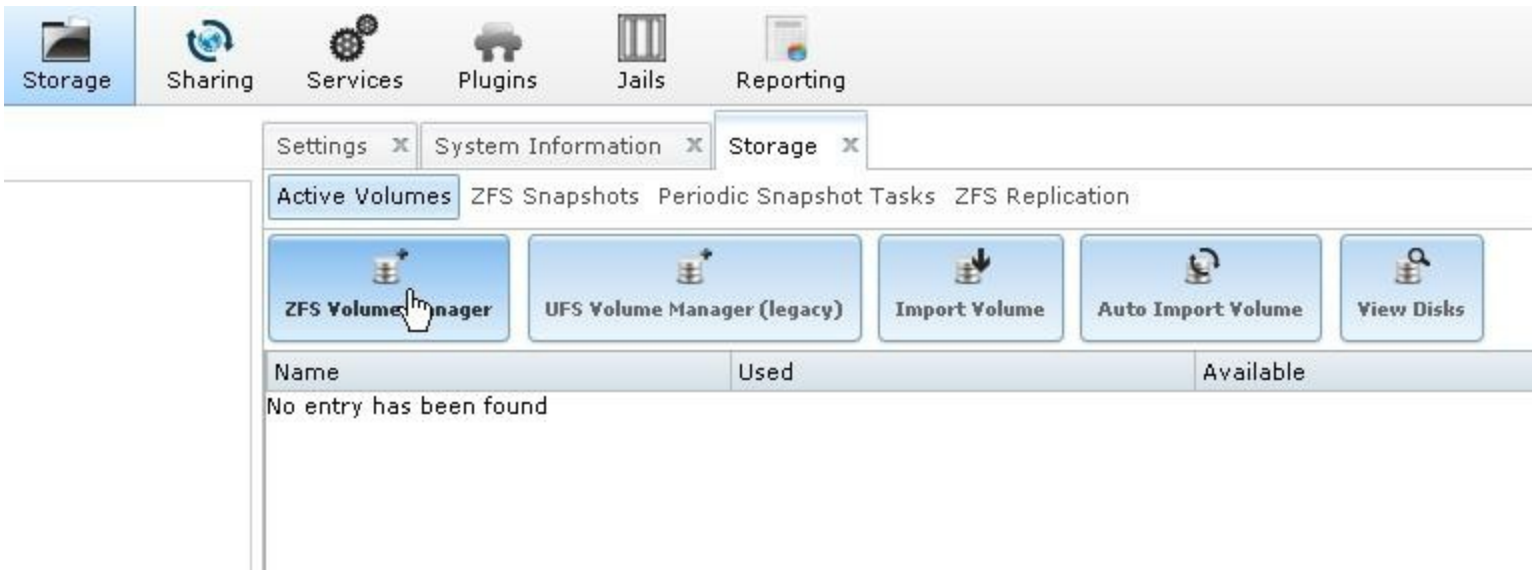
The **Add Group** dialog should then appear(shown below). Enter the new Group information as required.



3.11-Add A ZFS Volume

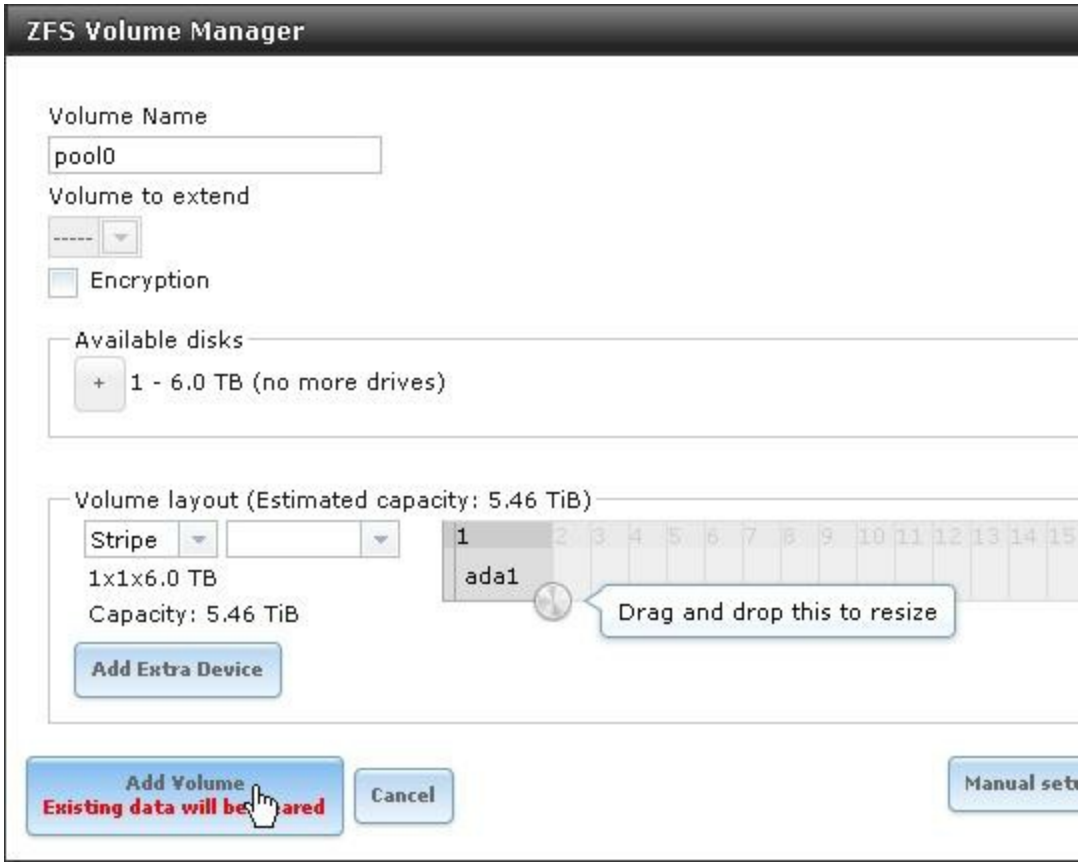
The freeNAS web interface makes it quite easy to add storage. To access the Volume Manager make sure you are working under the Storage tab at the top of the screen(pictured below).

To proceed: click **ZFS Volume Manager**



To add your new volume, type a unique name, then select the available disk(pictured below).

To proceed: click **Add Volume**



The new volume should then appear as active(shown below).

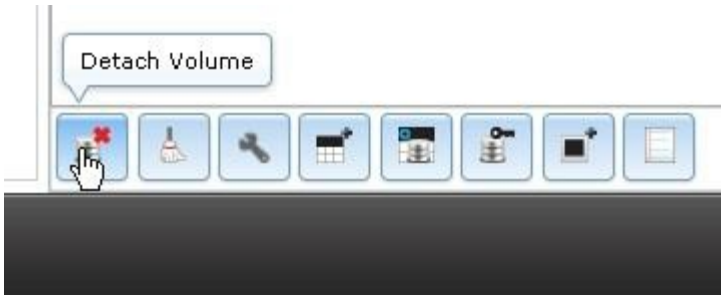
Active Volumes | ZFS Snapshots | Periodic Snapshot Tasks | ZFS Replication

Name	Used	Available
pool0	152.0 KiB (0%)	5.4 TiB

3.12-Detach And Move Volumes

If for some reason you need to ***move*** the freeNAS VM to another ***physical*** Proxmox machine the best method is to detach the volume ***cleanly***. At the bottom of the page you will see a set of control buttons(pictured below).

To proceed: click **Detach Volume**



freeNAS will then ask if you wish to destroy the data(pictured below)! **MAKE SURE YOU DO NOT CHECK THIS BOX OR YOUR DATA WILL BE GONE!**

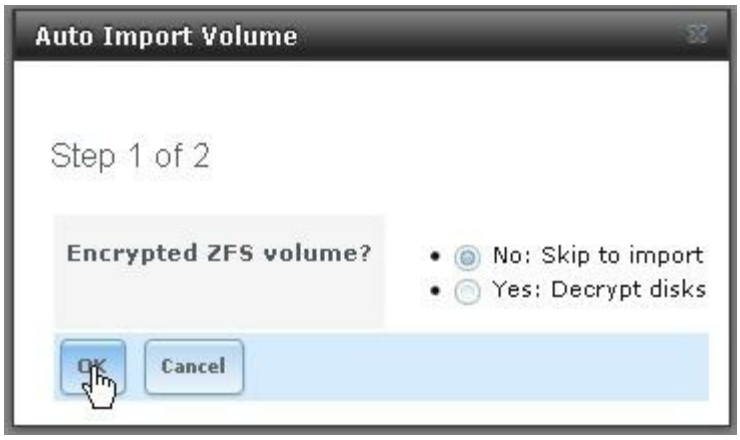
To proceed: click **Yes**

Once the volume is removed it should **NOT** be viewable under active volumes. Now you will want to shut down the freeNAS VM. I suggest making an additional **VM image backup** through the Proxmox interface. Make sure the backup is stored where it can be ***easily*** retrieved! Now you can safely power down the physical Proxmox machine and move the freeNAS data disks to your new Proxmox server.

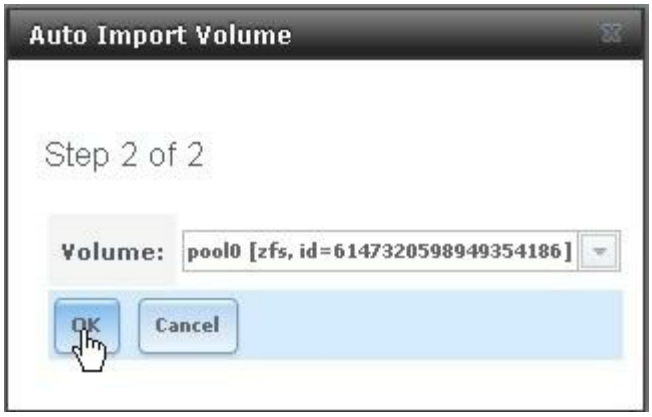
Once you are finished moving the data disks you'll need to restore the freeNAS VM backup image made prior to the move. The next step will be to re-add the hard disk pass-through on the new Proxmox server. If you forgot how go here:

Once you've completed the above steps power on the freeNAS VM, login, and click **Auto Import Volume**(pictured below).

You will now see the volume import wizard. In step 1 select No: Skip to import then click **OK**(shown below).



In step 2 select the volume you wish to import then click **OK**(shown below).



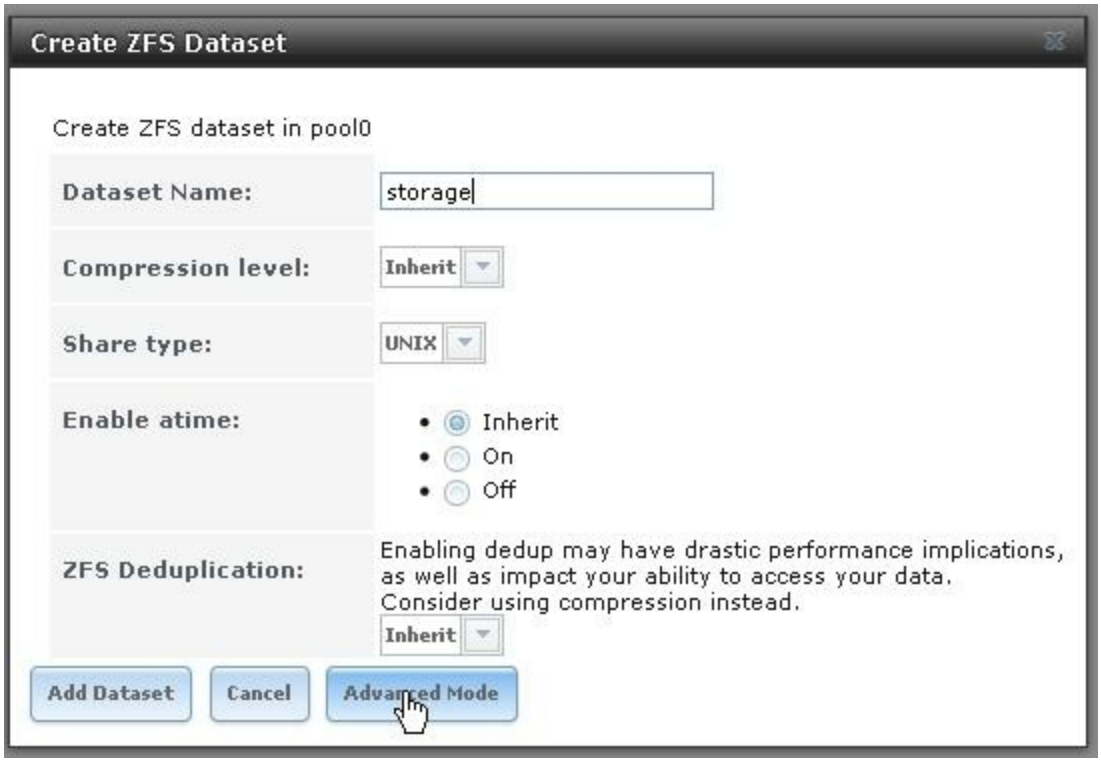
You should now see the volume showing active after a successful import(shown below).

3.13-ZFS Datasets

Now that we have created a volume it's time to refine it. The Dataset can be thought of similar to a folder in MS Windows. Better yet! A virtual folder with special properties!

To create a new Dataset: click **Create ZFS Dataset**(shown below)

The default view in freeNAS is ***Basic Mode*** so after you **name** the new dataset click the ***Advanced Mode*** button(shown below).



Advanced Mode offers refinements such as compression, share type, quota, reservation, and deduplication. **Notice** that I have set a 100 Gigabyte **quota** for this dataset(pictured below).

To proceed: click **Add Dataset**

Create ZFS Dataset

Create ZFS dataset in pool0

Dataset Name:	storage
Compression level:	Inherit
Share type:	UNIX
Enable atime:	• Inherit • On • Off
Quota for this dataset:	100g
Quota for this dataset and all children:	100g
Reserved space for this dataset:	0
Reserved space for this dataset and all children:	0
ZFS Deduplication:	Enabling dedup may have drastic performance implications, as well as impact your ability to access your data. Consider using compression instead. Inherit
Record Size:	Inherit

Add Dataset | Cancel | Basic Mode

You will now see your new dataset in the Active Volumes list(shown below). Notice the Size and Available column information comes from the quota set previously.

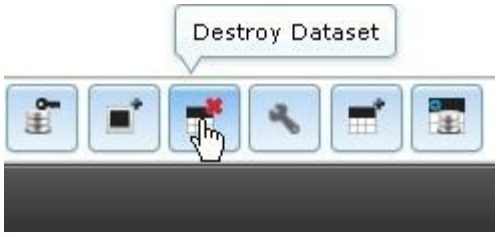
Active Volumes | ZFS Snapshots | Periodic Snapshot Tasks | ZFS Replication

ZFS Volume Manager | UFS Volume Manager (legacy) | Import Volume | Auto Import Volume | View Disks

Name	Used	Available	Size
pool0	160.0 KiB (0%)	5.4 TiB	5.4 TiB
storage	144.0 KiB (0%)	100.0 GiB	100.0 GiB

The above example shows a dataset name that I would **NOT** normally use. We will now destroy the dataset for reference.

To proceed: click **Destroy Dataset**(pictured below)



freeNAS developers wisely decided to give every opportunity to opt out of destructive actions. Notice the dialog with a Red background(pictured below).

I have provided a pre-populated volume with dataset naming conventions that I prefer to use. The ds prefix simply indicates that I am working with a dataset under the volume named pool0. Notice that it is possible to nest the datasets within other datasets(pictured below).

Active Volumes | ZFS Snapshots | Periodic Snapshot Tasks | ZFS Replication

ZFS Volume Manager | UFS Volume Manager (legacy) | Import Volume | Auto Import Volume | View Disks

Name	Used	Available	Size	Compression
pool0	200.0 KiB (0%)	2.4 TiB	2.4 TiB	lz4
ds.backups	160.0 KiB (0%)	151.9 GiB	151.9 GiB	lz4
ds.backups/websites	144.0 KiB (0%)	10.0 GiB	10.0 GiB	lz4
ds.backups/win7pro	348.1 GiB (69%)	151.9 GiB	500.0 GiB	lz4
ds.filestore	160.0 KiB (0%)	237.3 GiB	237.3 GiB	lz4
ds.filestore/protected	851.2 GiB (85%)	147.7 GiB	998.9 GiB	lz4
ds.filestore/public	99.8 GiB (52%)	89.6 GiB	189.4 GiB	lz4
ds.home	168.0 KiB (0%)	106.5 GiB	106.5 GiB	lz4
ds.home/administrator	144.0 KiB (0%)	20.0 GiB	20.0 GiB	lz4
ds.home/dbrewer	144.0 KiB (0%)	20.0 GiB	20.0 GiB	lz4
ds.home/lsurber	92.5 GiB (77%)	26.5 GiB	119.0 GiB	lz4
ds.iscsitrgts	168.0 KiB (0%)	445.9 GiB	445.9 GiB	lz4
ds.iscsitrgts/example.trgt012	172.0 KiB (0%)	40.0 GiB	40.0 GiB	lz4
ds.iscsitrgts/gameserver.trgt013	30.7 GiB (15%)	169.3 GiB	200.0 GiB	lz4
ds.iscsitrgts/win7pro.trgt1	273.5 GiB (68%)	126.5 GiB	400.0 GiB	lz4
ds.mediaserver	160.0 KiB (0%)	317.0 GiB	317.0 GiB	lz4
ds.mediaserver/music	286.0 GiB (71%)	113.8 GiB	399.8 GiB	lz4
ds.mediaserver/video	676.7 GiB (84%)	123.3 GiB	800.0 GiB	lz4
ds.proxmox	192.0 KiB (0%)	439.2 GiB	439.2 GiB	lz4
ds.proxmox/nfs.containers	160.0 KiB (0%)	40.0 GiB	40.0 GiB	lz4
ds.proxmox/nfs.images	152.0 KiB (0%)	40.0 GiB	40.0 GiB	lz4
ds.proxmox/nfs.isostore	33.8 GiB (42%)	46.2 GiB	80.0 GiB	lz4
ds.proxmox/nfs.netbackups	325.4 GiB (54%)	274.6 GiB	600.0 GiB	lz4
ds.proxmox/nfs.netbackups2	400.6 MiB (19%)	1.6 GiB	2.0 GiB	lz4
ds.proxmox/nfs.templates	1.3 GiB (3%)	38.7 GiB	40.0 GiB	lz4

You can edit an existing dataset at any time. Let's look at the properties of the dataset named ds.filestore/protected (pictured below).

Active Volumes | ZFS Snapshots | Periodic Snapshot Tasks | ZFS Replication

ZFS Volume Manager | UFS Volume Manager (legacy) | Import Volume | Auto Import Volume | View Disks

Name	Used	Available	Size
pool0	192.0 KiB (0%)	2.8 TiB	2.8 TiB
ds.backups	152.0 KiB (0%)	151.9 GiB	151.9 GiB
ds.backups/win7pro	348.1 GiB (69%)	151.9 GiB	500.0 GiB
ds.filestore	160.0 KiB (0%)	246.6 GiB	246.6 GiB
ds.filestore/protected	847.2 GiB (84%)	151.5 GiB	998.7 GiB
ds.filestore/public	104.0 GiB (52%)	95.0 GiB	199.1 GiB
ds.home	168.0 KiB (0%)	107.4 GiB	107.4 GiB
ds.iscsitrgts	160.0 KiB (0%)	445.5 GiB	445.5 GiB
ds.iscsitrgts/gameserver.trgt013	30.6 GiB (15%)	169.4 GiB	200.0 GiB
ds.iscsitrgts/win7pro.trgt1	273.8 GiB (68%)	126.2 GiB	400.0 GiB
ds.mediaserver	160.0 KiB (0%)	260.3 GiB	260.3 GiB
ds.mediaserver/music	286.0 GiB (71%)	113.7 GiB	399.7 GiB
ds.mediaserver/video	651.4 GiB (93%)	48.5 GiB	700.0 GiB

To view the dataset properties click **Edit ZFS Options**(shown below).

If you need additional space for this dataset change both quota values according to your needs(shown below).

Edit ZFS Options

Dataset: pool0/ds.filestore/protected

Compression level:	lz4 (recommended)
Share type:	UNIX
Enable atime:	• Inherit • On • Off
Quota for this dataset:	1000G
Quota for this dataset and all children:	1000G
Reserved space for this dataset:	0
Reserved space for this dataset and all children:	0
ZFS Deduplication:	Enabling dedup may have drastic performance implications, as well as impact your ability to access your data. Consider using compression instead. Inherit

Edit Dataset | Cancel | Basic Mode

Pay close attention NOT to exceed the size of the parent dataset(shown below)!

Edit ZFS Options

Dataset: pool0/ds.filestore

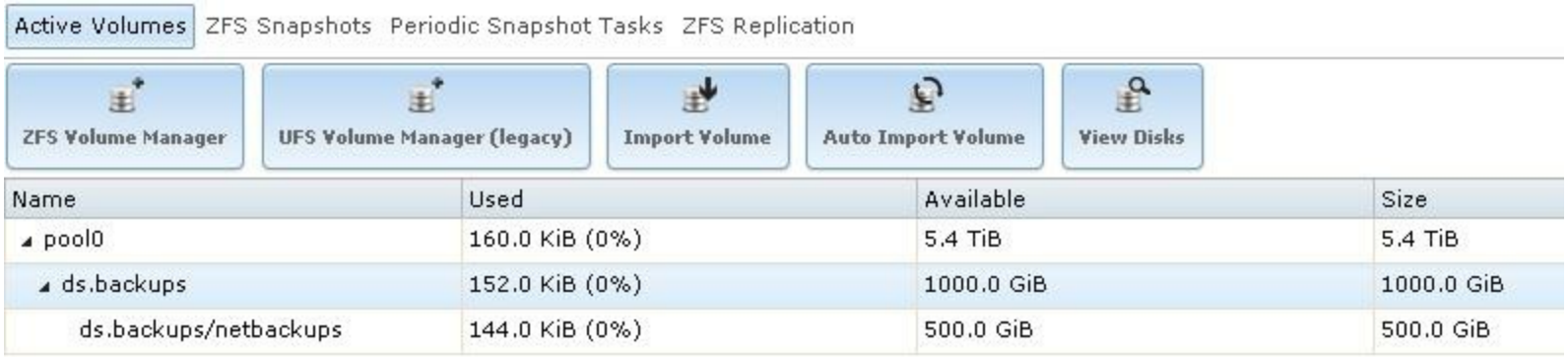
Compression level:	lz4 (recommended)
Share type:	UNIX
Enable atime:	• Inherit • On • Off
Quota for this dataset:	1.17T
Quota for this dataset and all children:	1.17T
Reserved space for this dataset:	0
Reserved space for this dataset and all children:	0
ZFS Deduplication:	Enabling dedup may have drastic performance implications, as well as impact your ability to access your data. Consider using compression instead. Inherit

Edit Dataset | Cancel | Basic Mode

3.14-ZFS Permissions

Generally, when you create a dataset you will need to set appropriate permissions for users. For the purpose of this example we will setup **public** permissions, which are **wide open**. No need to worry though, you can also **restrict** a public share by IP address under the **Shares** tab. I can say with confidence, even with public permissions set on your shares, ***so long as pfSense is setup according to this book***, using hardware filtering, that ***you are quite secure***!

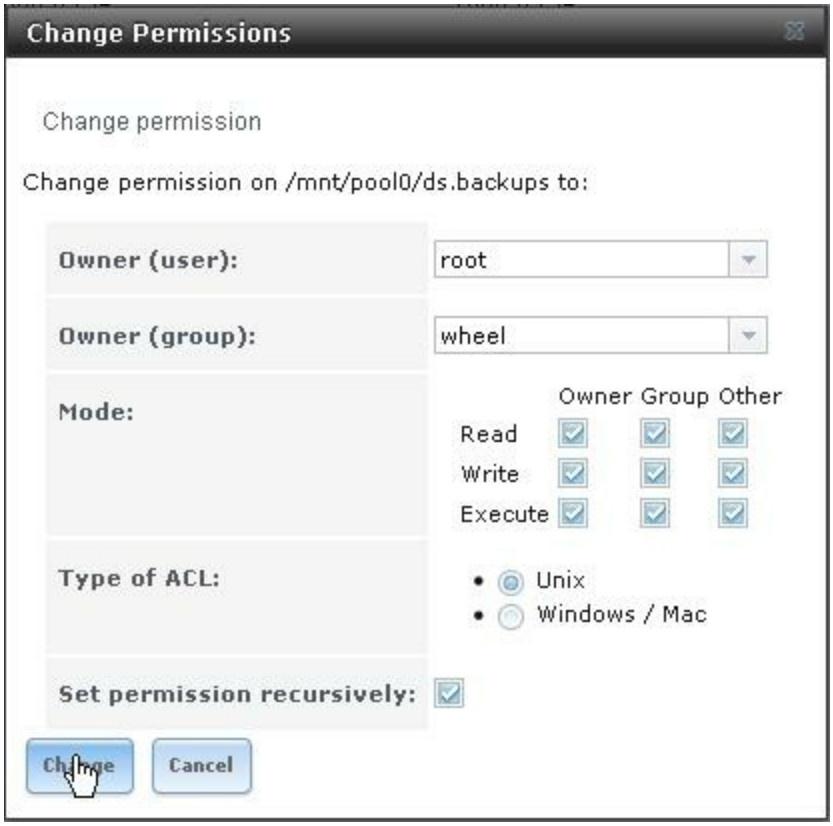
Let's set permissions on the ***ds.backups dataset*** now(pictured below).



To proceed: click **Change Permissions**(pictured below)

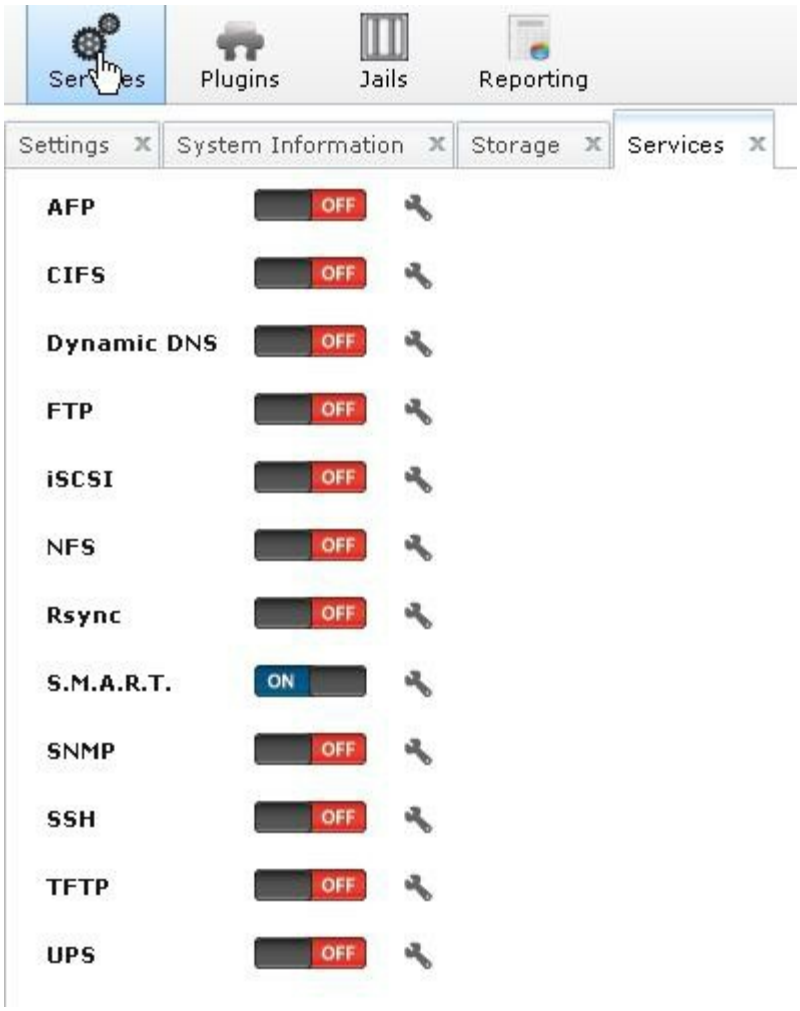
You should now see the Permissions dialog(pictured below). To enable public access to this dataset I have checked every box under **Mode** for ***Owner***, ***Group***, and ***Other***. The recursive check box means that **ALL** datasets ***nested*** under this one will have permissions changed as well. **ACL** can be left defaulted to Unix even if configured under a domain. If you need ***specific*** **user** or **group** privileges they can be selected using the dropdown box.

NOTE: If you have trouble connecting to a share this is where you start your troubleshooting. Resetting permissions as shown below will guarantee access to the dataset.


Change Permissions
Change permission
Change permission on /mnt/pool0/ds.backups to:
Owner (user):
root
Owner (group):
wheel
Mode:
Owner Group Other
Read
Write
Execute
Type of ACL:
Unix
Windows / Mac
Set permission recursively:
Change
Cancel

3.15-freeNAS Services

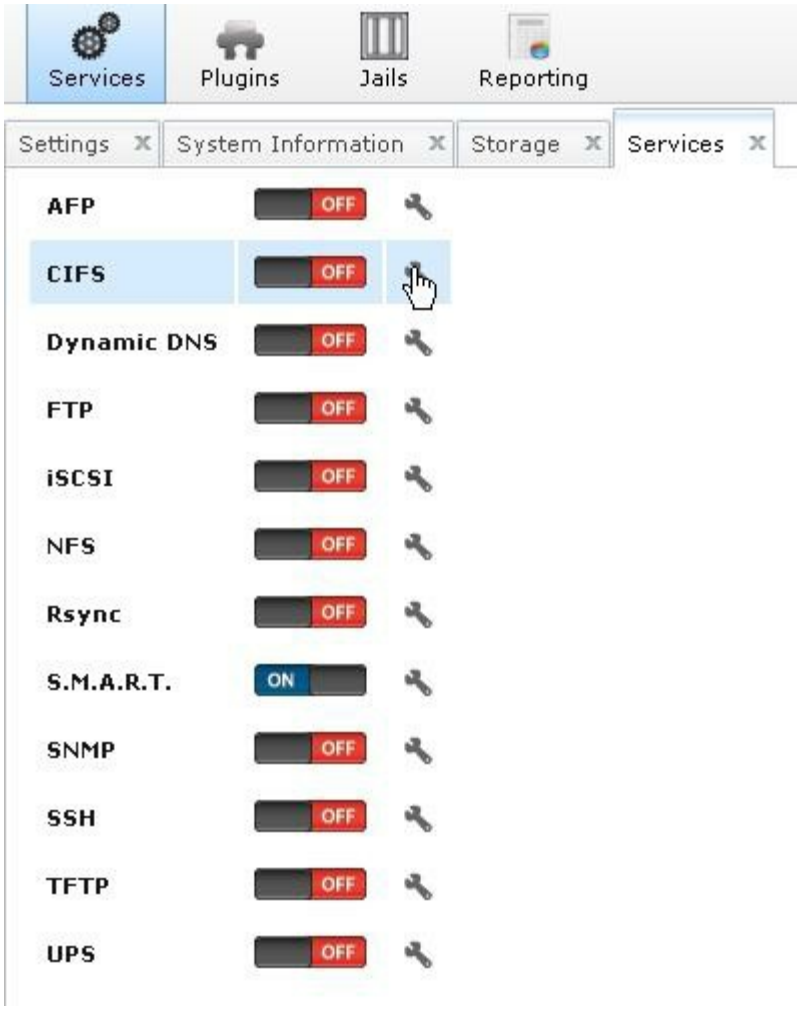
Your server can be setup to host a variety of services which can be found under the Services tab(pictured below). In this book we will be primarily concerned with **CIFS, iSCSI, NFS**, **Rsync, and SSH**.



3.15.1-CIFS(Windows Sharing) Service

First we'll look at **CIFS**(otherwise known as **SAMBA**). This service is the backbone of ***Windows compatible*** networks and will be your primary file sharing protocol. Let's look at the configuration options for **CIFS** now.

To proceed: click the **wrench icon**(shown below)



The default configuration options(pictured below) will allow sharing of files in a Windows network as a ***computer named freenas*** within the ***Workgroup named WORKGROUP***. You will need to change these names according to your needs! For example: My domain name is called **yourwebs.us** and my workgroup is called **YOURWEBS**. Because I have more than one **freeNAS** server running I use names such **as freeNAS-1**, **freeNAS-2**, **freeNAS-3**, etc.

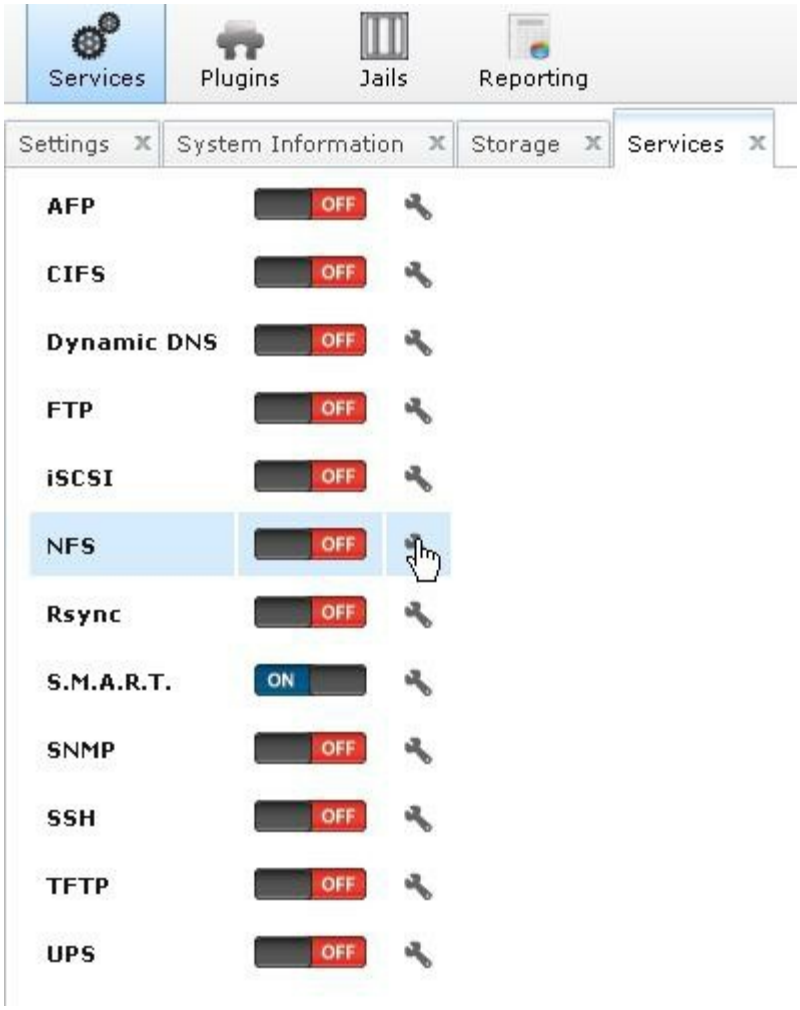
CIFS Settings

NetBIOS name:	freenas
Workgroup:	WORKGROUP
Description:	FreeNAS Server
DOS charset:	CP437
UNIX charset:	UTF-8
Log level:	Minimum
Use syslog:	☐
Local Master:	☑
Time Server for Domain:	☑
Guest account:	nobody
File mask:	
Directory mask:	
EA Support:	☐
Support DOS File Attributes:	☑
Allow Empty Password:	☐
Auxiliary parameters:	

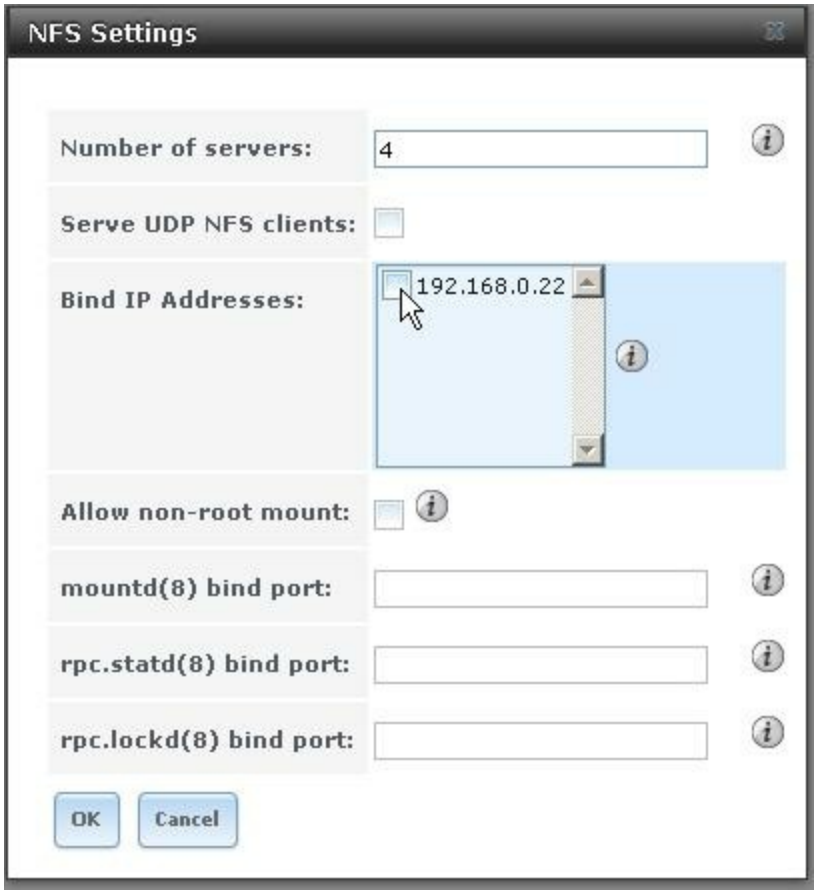
3.15.2-NFS(Linux Sharing) Service

Next, we'll look at **NFS**. This service is the original Linux based file sharing protocol. Today you can install services on windows to connect to **NFS** shares. I prefer to keep my **NFS** shares locked down to only Linux machines. If you need windows access just enable a temporary CIFS share that only you have permissions for. Let's look at the configuration options for **NFS** now.

To proceed: click the **wrench icon**(shown below)



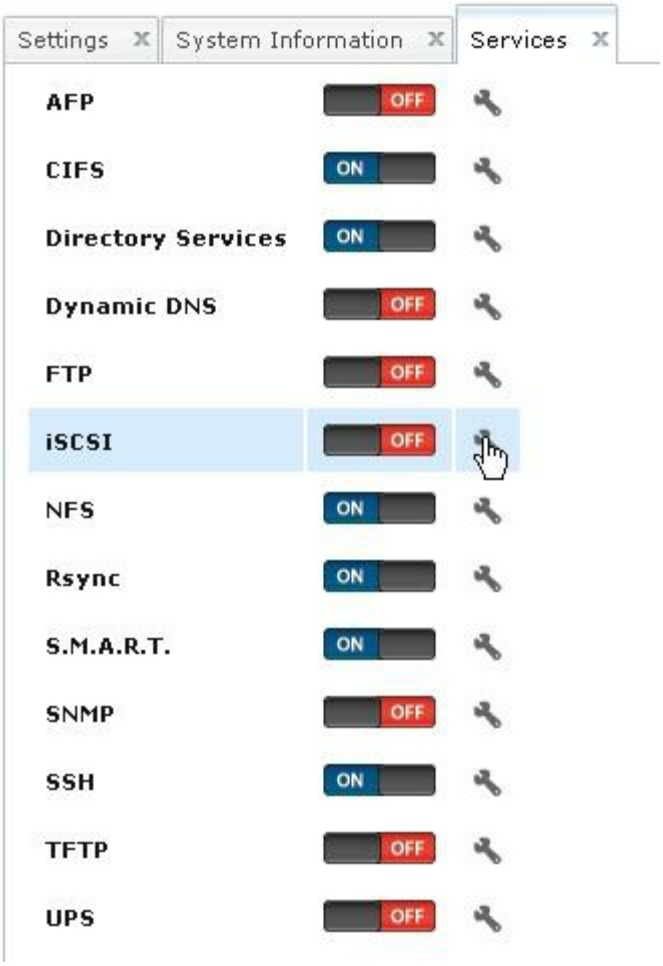
The only configuration option that you will ever need to change is the **Bind IP Address**(shown below). It is possible to bind NFS to a different IP than that used for CIFS shares. For best performance I recommend having 2 network adapters, one for CIFS and the other for NFS and Rsync.



3.15.3-iSCSI Target Service

Next, we'll look at iSCSI Global options. iSCSI is a powerful networking protocol and can be a little challenging to beginners. It allows serialized shares to be created in such a way that the guest operating system is fooled into believing it has multiple physical drives. Let's look at the Global Configuration options for **iSCSI** now.

To proceed: click the **wrench icon**(shown below)



You should now see the Target Global Configuration screen as shown below. The only thing on this screen that you should touch would be the Base Name. For example: you may want to change ***org.example*** (pictured below) to something like ***us.freenas1.yourwebs***

CAUTION: Be careful when changing the Base Name or your server might not be visible for mapping. If this happens revert back to default: iqn.2011-03.org.example.istgt

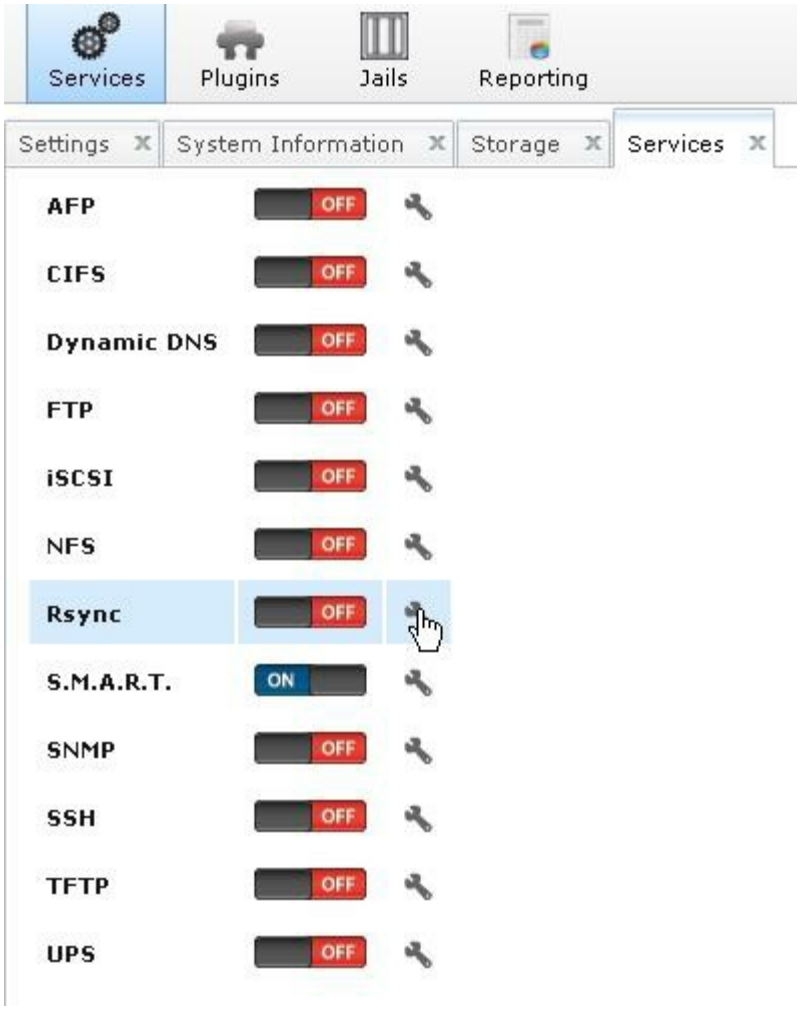
Target Global Configuration | Portals | Initiators | Authorized Access | Targets | Extents | Associated Targets

Base Name:	iqn.2011-03.org.example.ist
Discovery Auth Method:	None
Discovery Auth Group:	None
I/O Timeout:	30
NOPIN Interval:	20
Max. sessions:	16
Max. connections:	8
Max. pre-send R2T:	32
MaxOutstandingR2T:	16
First burst length:	65,536
Max burst length:	262,144
Max receive data segment length:	262,144
DefaultTime2Wait:	2
DefaultTime2Retain:	60
Enable LUC:	
Controller IP address:	127.0.0.1
Controller TCP port:	3261
Controller Authorized Network:	127.0.0.0/8
Controller Auth Method:	CHAP

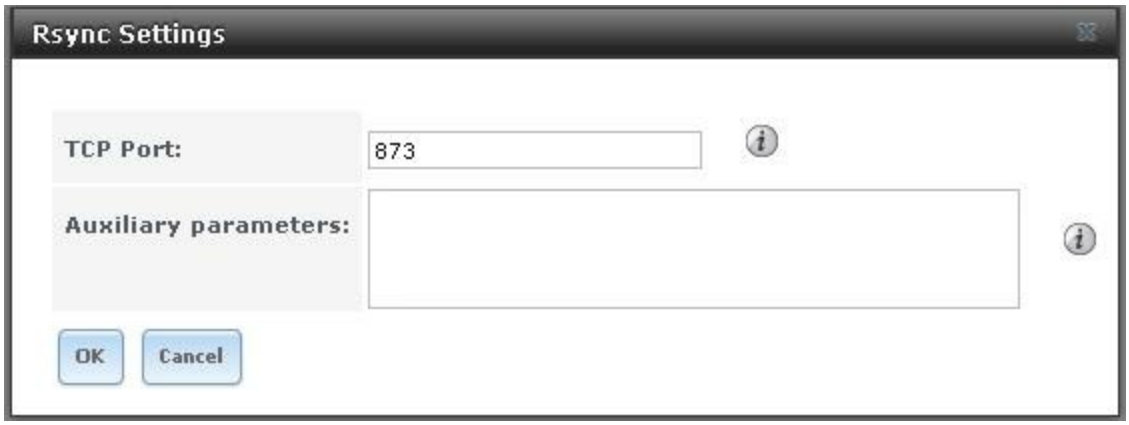
3.15.4-Rsync(Backup) Service

Now, we'll look at Rsync configuration options. Rsync is a powerful backup utility which is widely used in the Linux community. It is light weight and very good at what it does! freeNAS provides excellent scripting for Rsync backups! We'll cover that later! Let's look at the configuration options for **Rsync** now.

To proceed: click the **wrench icon**(shown below)



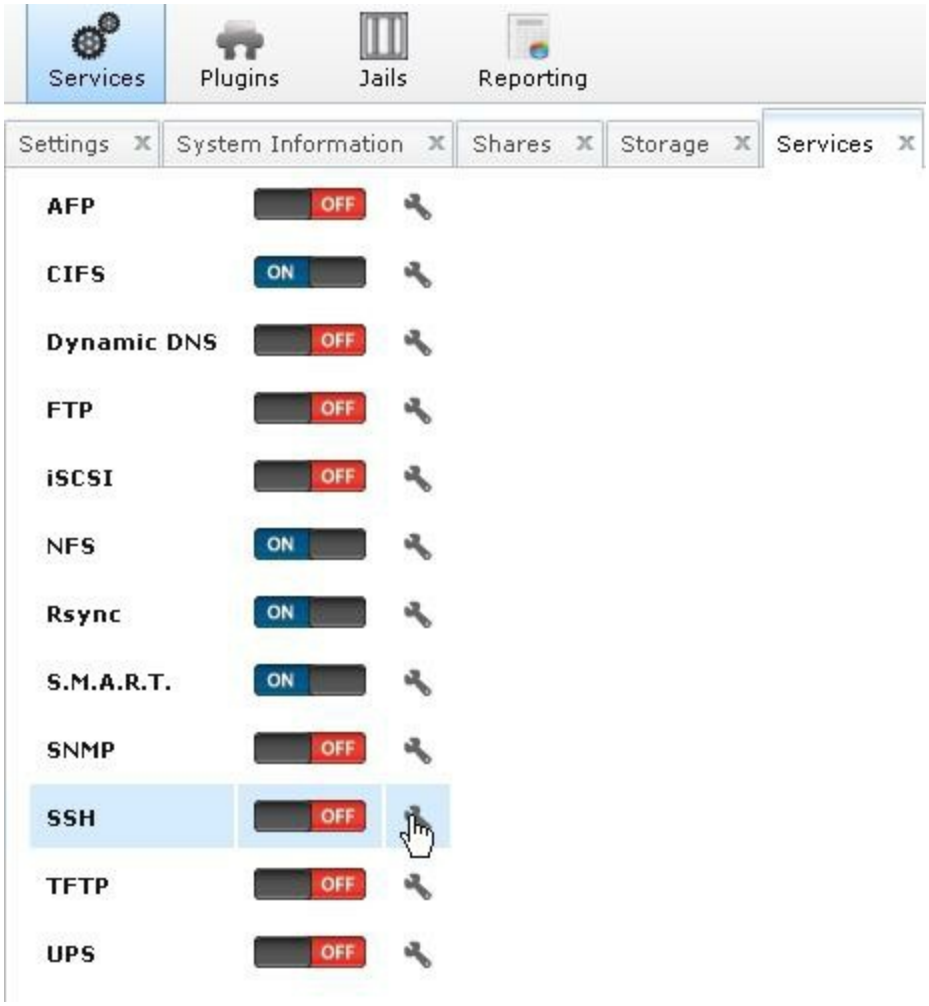
The configuration for the Rsync service is simple. There really isn't any! Keep the default TCP port value(pictured below).



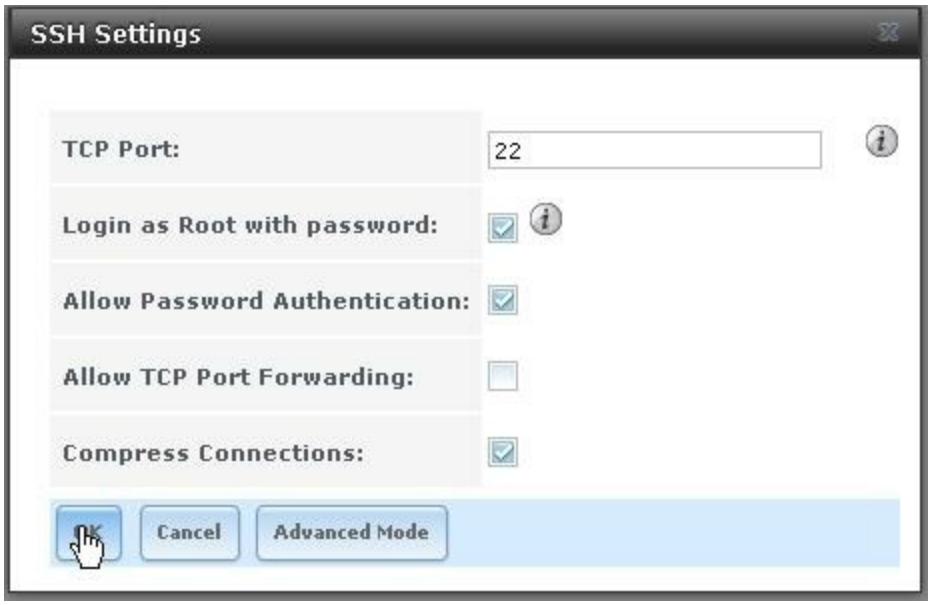
3.15.5-SSH(Secure Shell) Service

Finally, we'll look at SSH configuration options. SSH stands for secure shell. It allows remote logins via a console program such as the PuTTY program used earlier in the book. Let's look at the configuration options for **SSH** now.

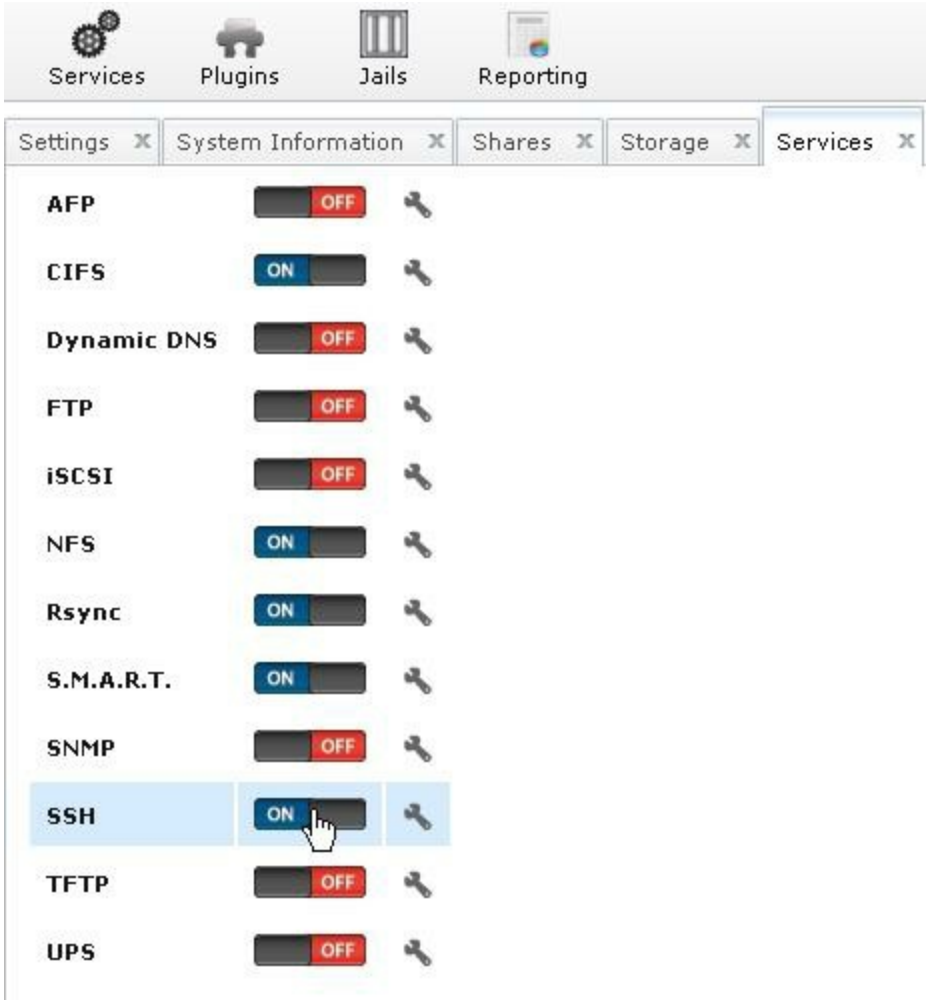
To proceed: click the **wrench icon**(shown below)



Make sure to match ALL checkboxes that I have checked(pictured below). No further configuration is needed.



Now that we've covered the important service configuration options make sure they're all enabled by clicking each of the service switches(shown below). They should turn blue when enabled!


Services
Plugins
Jails
Reporting
Settings
System Information
Shares
Storage
Services
AFP
OFF
CIFS
ON
Dynamic DNS
OFF
FTP
OFF
iSCSI
OFF
NFS
ON
Rsync
ON
S.M.A.R.T.
ON
SNMP
OFF
SSH
ON
TFTP
OFF
UPS
OFF

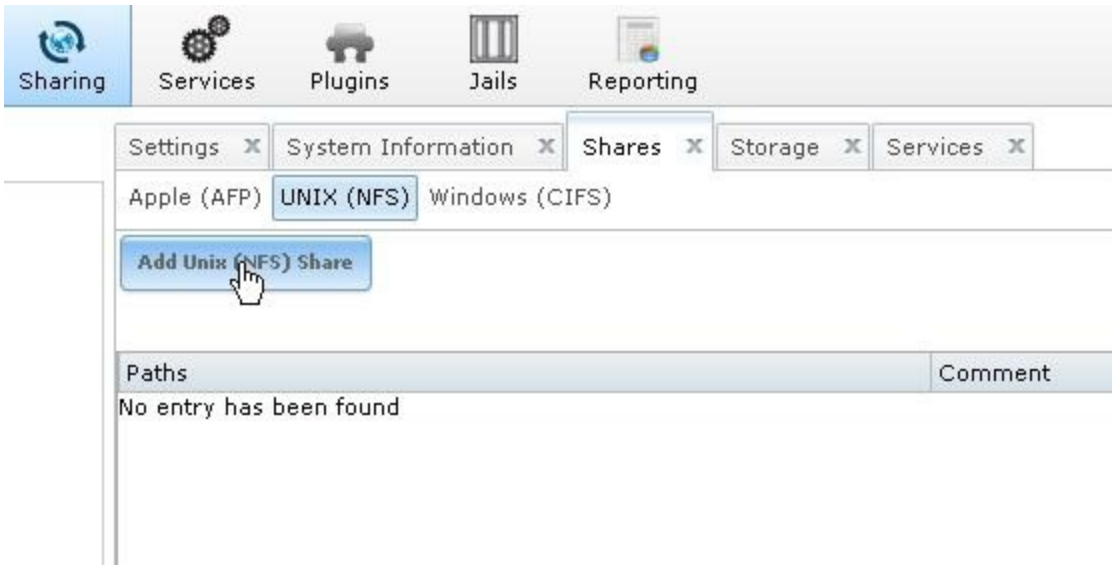
3.16-Add Network Shares

3.16.1-NFS Shares

As mentioned earlier in the book, I prefer to use NFS shares for Proxmox backups. We will now create a share called ***netbackups*** which will be used for ***Proxmox VM image backups***.

To proceed click **Sharing>NFS**(pictured below)

Next, click **Add NFS Share**(pictured below).



When the dialog appears type in the appropriate information(pictured below). Notice that I have **Authorized** 3 Proxmox server IP addresses. This will restrict access and is strongly suggested! Under **Maproot User** select root. This may **NOT** be the most secure but is **guaranteed** to work and keeps things simple. Also notice that I have browsed and selected a ***nested dataset*** under **ds.backup** named **netbackups**.

If you have not created a dataset yet go back a do so now. Otherwise, click close after your dataset selection(pictured below).

Add Unix (NFS) Share

Comment: proxmox nfs netbackups

Authorized networks:

Authorized IP addresses or hosts:
192.168.0.16
192.168.0.2
192.168.0.6

All Directories:

Read Only:

Quiet:

Maproot User: root

Maproot Group: N/A

Mapall User: N/A

Mapall Group: N/A

Path

Path: /mnt/pool0/ds.backups/netb

Close

/
mnt
pool0
ds.backups
netbackups

Now, carefully review your entries then click **OK** to proceed(pictured below).

Add Unix (NFS) Share

Comment:	proxmox nfs netbackups
Authorized networks:	
Authorized IP addresses or hosts:	192.168.0.16 192.168.0.2 192.168.0.6
All Directories:	☐
Read Only:	☐
Quiet:	☑
Maproot User:	root
Maproot Group:	N/A
Mapall User:	N/A
Mapall Group:	N/A

Path

Path: /mnt/pool0/ds.backups/netb Browse

Add extra Path

OK Cancel

You should now see the new NFS netbackups share in the list(pictured below).

Apple (AFP) UNIX (NFS) Windows (CIFS)

Add Unix (NFS) Share

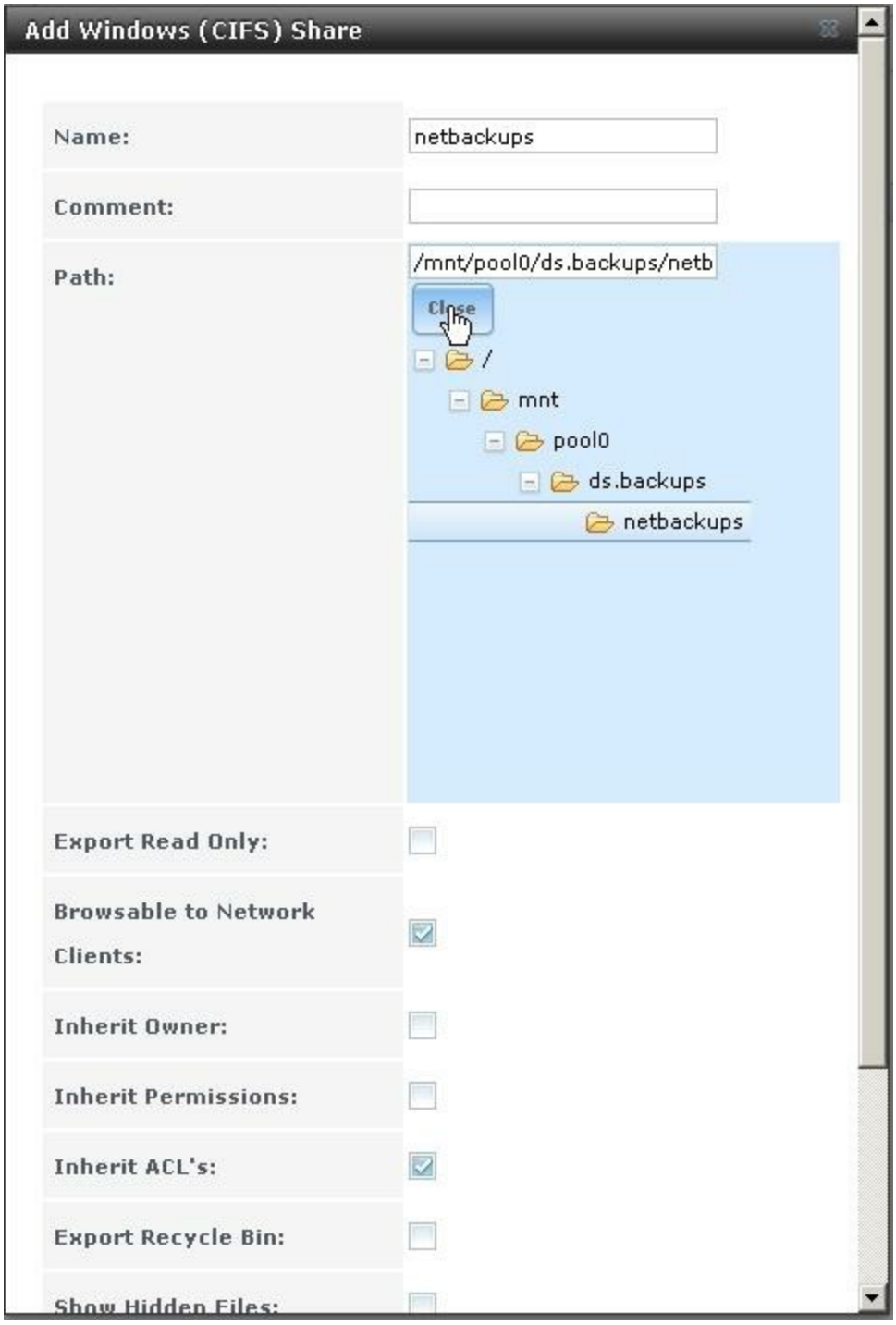
Paths	Comment
/mnt/pool0/ds.backups/netbackups	proxmox nfs netbackups

3.16.2-Windows Shares

Setting up a Windows share is very similar to NFS. We will now create a share called ***netbackups*** which can be used to access ***Proxmox VM image backups*** from Windows.

To proceed: click **Add CIFS Share**(pictured below).

Start by typing an appropriate **Name** and selecting the dataset **Path** as shown below!



Now, enter a comment if you wish and set all other options according to your needs. Notice that I have set this share to **Read Only** and **Browsable to Network Clients**(shown below).

Add Windows (CIFS) Share

Name:	netbackups
Comment:	netbackups
Path:	/mnt/pool0/ds.backups/netb Browse
Export Read Only:	☑
Browsable to Network Clients:	☑
Inherit Owner:	☐
Inherit Permissions:	☐
Inherit ACL's:	☑
Export Recycle Bin:	☐
Show Hidden Files:	☐
Allow Guest Access:	☐
Only Allow Guest Access:	☐

OK Cancel Advanced Mode

Once finished, your new Windows share will be visible in the list(pictured below).

Apple (AFP) UNIX (NFS) Windows (CIFS)

Add Windows (CIFS) Share

Name	Comment	Path
netbackups	netbackups	/mnt/pool0/ds.backups/netbackups

3.16.3-iSCSI Target Shares

I have elected to save **iSCSI** for last because it takes the most time to configure. Please pay attention closely! To setup an **iSCSI** target you'll first need to ***add a dataset*** to be mapped. For this example I have created a 40Gb dataset named **example.trgt012** nested within the **ds.iscsitrgts** dataset(pictured below). This naming convention helps me identify the intended type of share I'm working with.

Create ZFS Dataset

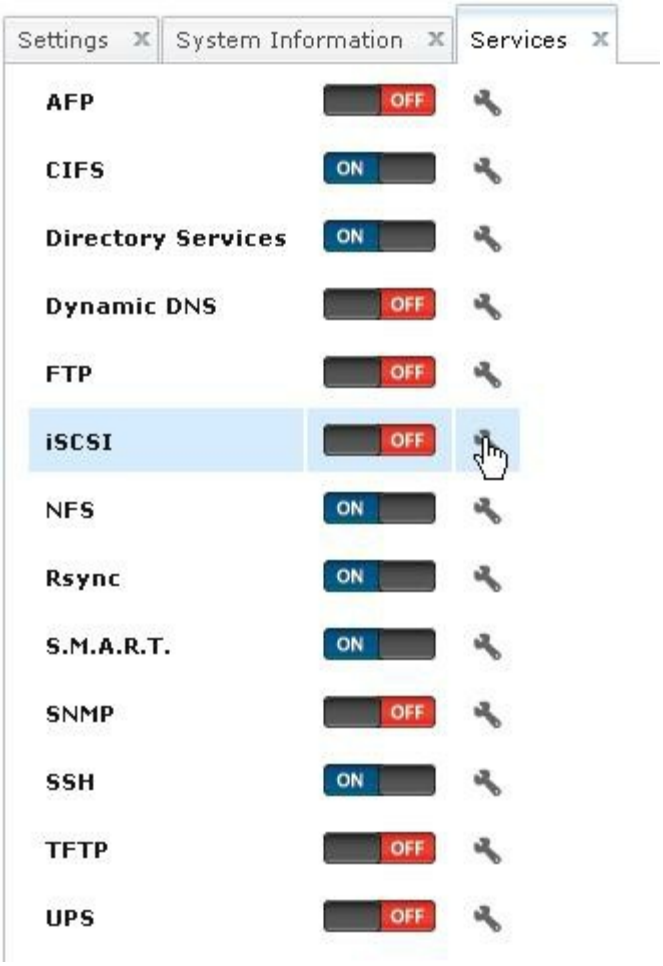
Create ZFS dataset in pool0/ds.iscsitrgts

Dataset Name:	example.trgt012
Compression level:	Inherit
Share type:	UNIX
Enable atime:	• Inherit • On • Off
Quota for this dataset:	40g
Quota for this dataset and all children:	40g
Reserved space for this dataset:	0
Reserved space for this dataset and all children:	0
ZFS Deduplication:	Enabling dedup may have drastic performance implications, as well as impact your ability to access your data. Consider using compression instead. Inherit
Record Size:	Inherit

Add Dataset | Cancel | Basic Mode

Once you have created a dataset go to the Services tab as shown below.

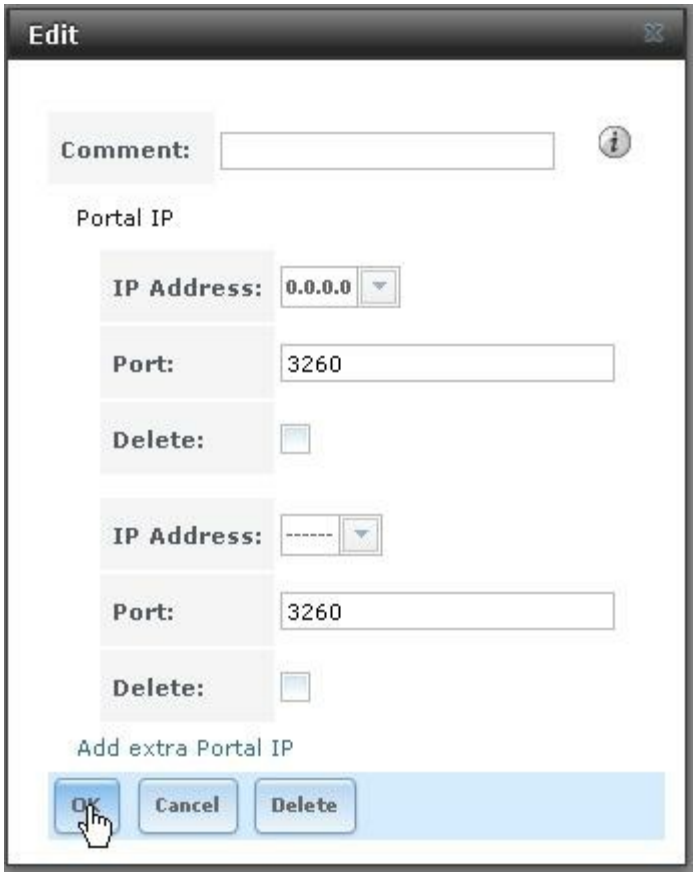
To proceed: click the **wrench icon**(shown below)



Next go straight to the **Portals** tab then click **Add Portal**(shown below)

When the dialog screen appears(shown below) you will notice the default **IP Address** is set to **0.0.0.0** implying that **ANY** interface will be used. This setting is fine! You may also wish to add a comment.

To proceed: click **OK**



Next, we'll setup Initiators! To proceed: click **Add Initiator**(shown below)

You should now see the Add Initiator dialog(pictured below). Since you are in a Layer 2 hardware protected network it is safe to keep the default settings.

To proceed: click **OK** (shown below)

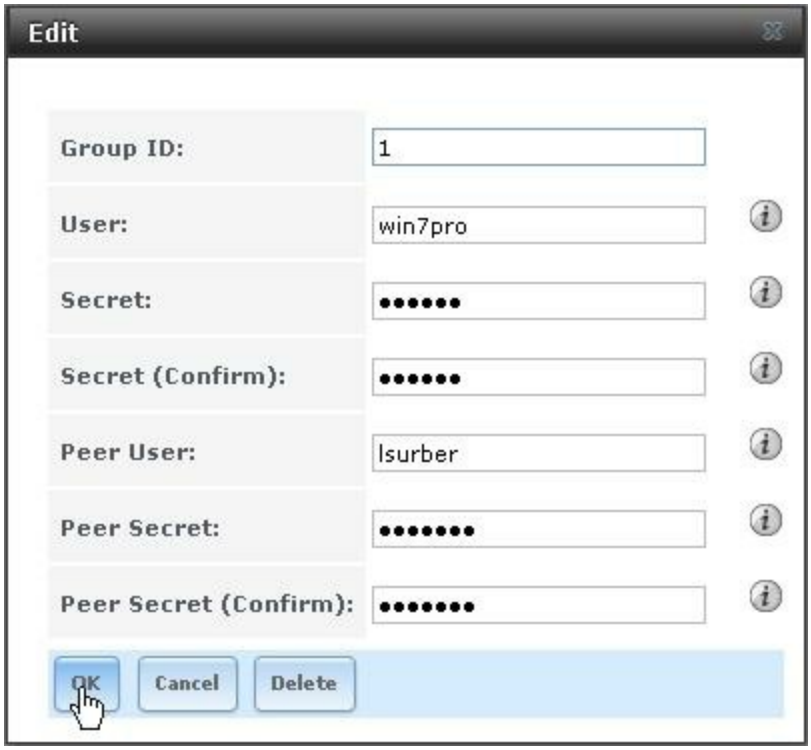
Now we'll setup Access Groups!

To proceed: click **Add Authorized Access**(shown below)

When the dialog appears as shown below enter the appropriate information. For this example I have set the **User** as a ***network client*** named **win7pro** and the **Peer User** as my ***active directory Username***: **lsurber**

NOTE: The **Secret** and **Peer Secret** cannot be the same! I choose an ***arbitrary*** **Secret** while using my ***active directory password*** for the **Peer Secret**.

To proceed: click **OK**(shown below)



Next up is Targets! To proceed: click Add **Target**(shown below)

You should now see the Target Dialog screen shown below. My preference is to use the name of the dataset(example.trgt012) as the Target Name. Now, select the **Portal Group ID** and the **Initiator Group ID** establish earlier. You could also choose an **Authentication Group number**. I have left this set to none for this example.

To proceed: click **OK**(pictured below)

Add Target

Target Name:	example.trgt012
Target Alias:	
Serial:	7aa96c6a308d02
Target Flags:	read-write
Portal Group ID:	1
Initiator Group ID:	1
Auth Method:	Auto
Authentication Group number:	None
Queue Depth:	32
Logical Block Size:	512

OK Cancel

You should now see your newly created **Target** as shown below.

Target Global Configuration | Portals | Initiators | Authorized Access | Targets | Extents | Associated Targets

Add Target

Target Name	Target Alias	Serial	Target Flags	Portal Group ID
example.trgt012		7aa96c6a308d02	rw	1
torrentreaper.trgt013		7aa96c6a308d01	rw	1
win7pro.trgt1		7aa96c6a308d00	rw	1

Next we'll configure the Extent!

To proceed: click **Add Extent**(pictured below)

Target Global Configuration | Portals | Initiators | Authorized Access | Targets | Extents | Associated Targets

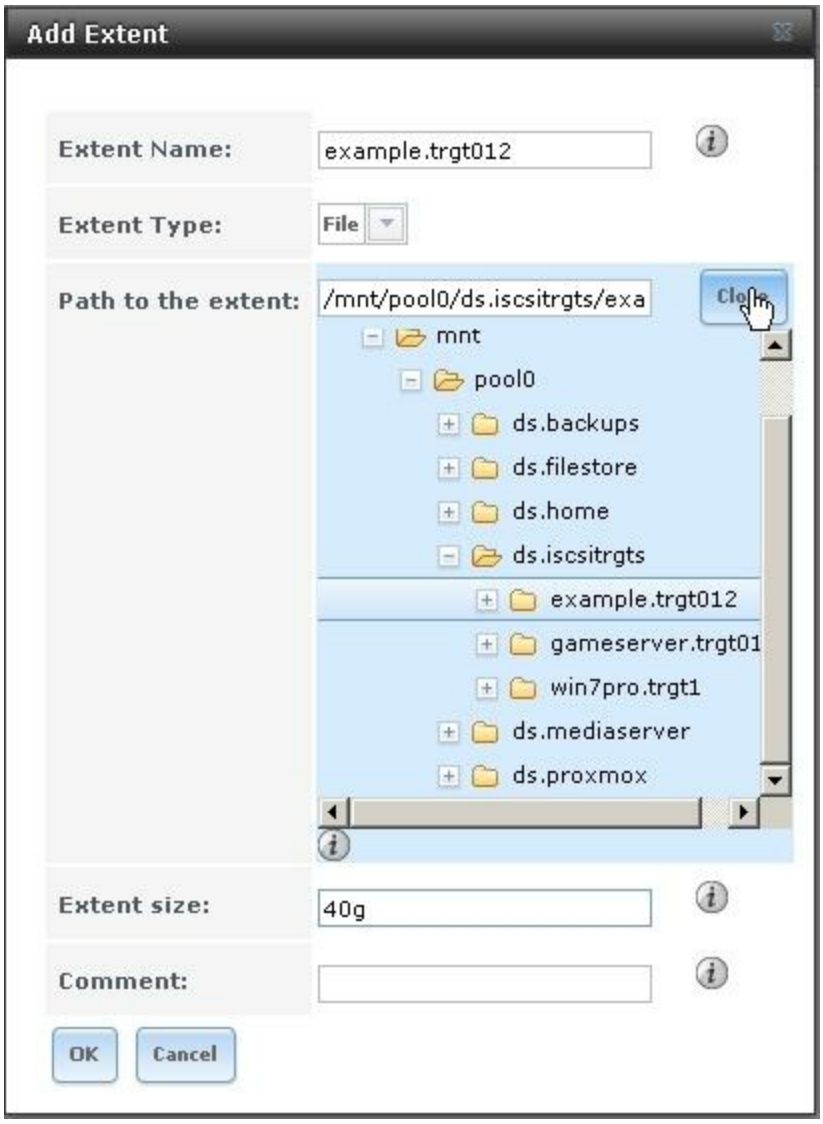
Add Extent

Extent Name	Extent Type	Path to the extent	Comment
torrentreaper.trgt013	File	/mnt/pool0/ds.iscsitrgts/gameserver.trgt013/trgt013	TorrentReaper Target
win7pro.trgt1	File	/mnt/pool0/ds.iscsitrgts/win7pro.trgt1/trgt1	Win7Pro Target

Once again, I have chosen to use the dataset name for the Extent Name and set the **Extent size** to **40g**.

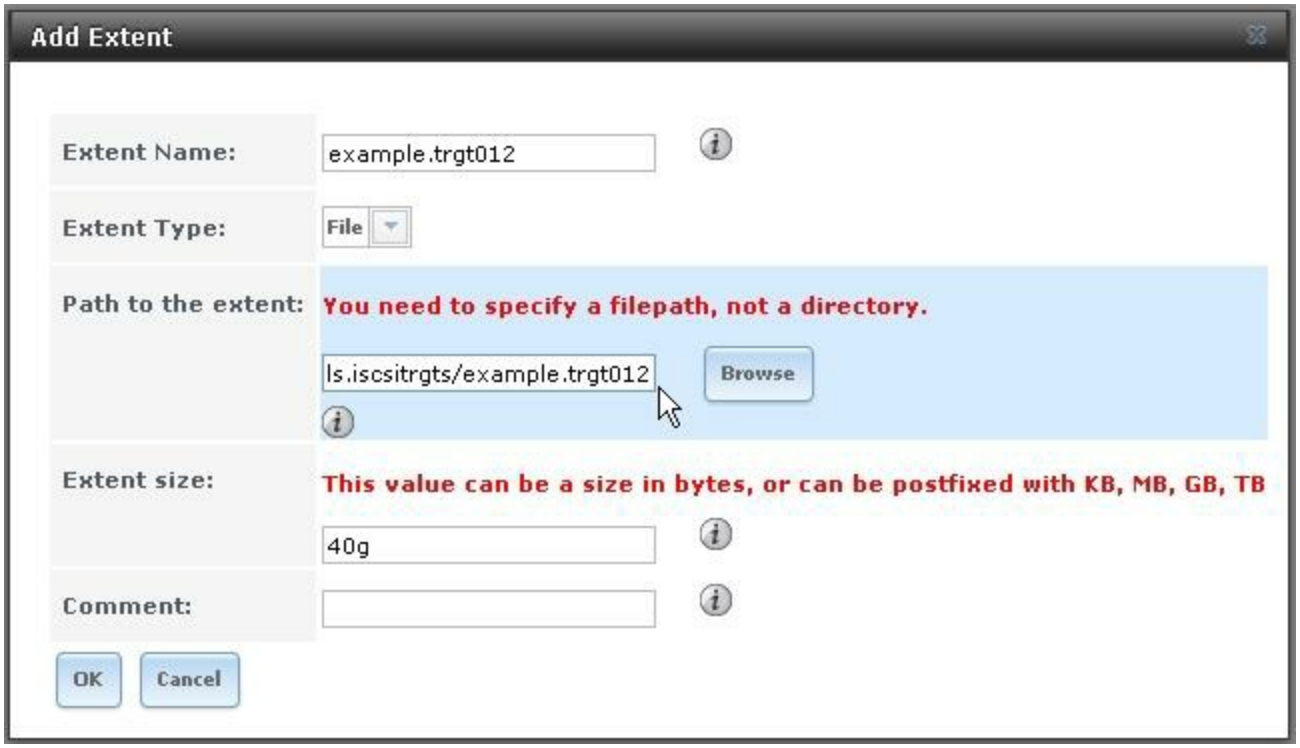
This matches the quota I set for the dataset when it was created. My preference and recommendation is to use the **File *Extent Type***. Now choose the appropriate **Path to the extent**. NOTICE: I have selected the nested dataset **example.trgt012** for the **path.**

After selecting your path: click **Close**(shown below)



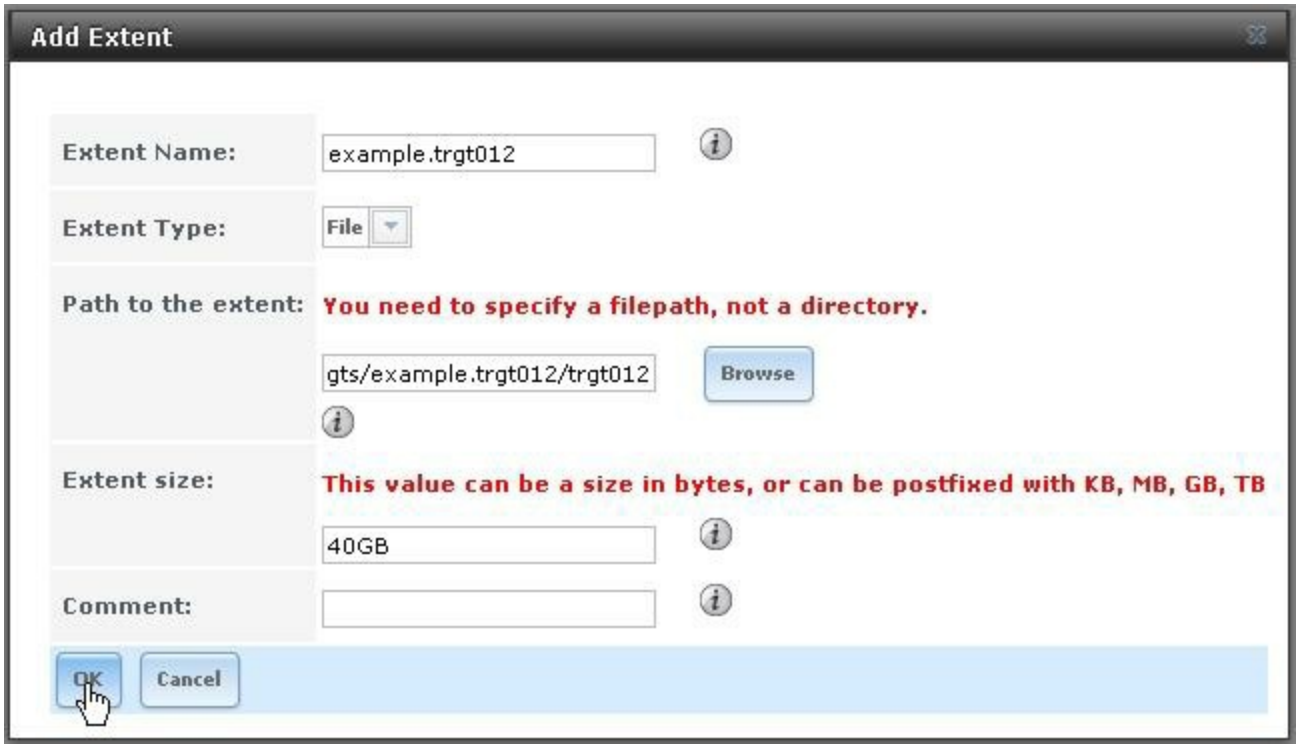
To proceed: click **OK**(shown below)

I have purposely created this ***common*** error for your reference(shown below). **NOTICE**: because this is a **File** Extent Type you cannot simply select the ***dataset*** as the **Path to the extent**. Also, notice the correct **Extent size *syntax*** was wrong! It should have been **40GB**.



To ***correct*** the **Path to the extent** I will simply add **/trgt012** to the **end** of the **selected dataset**. You may be starting to understand why naming is important!

With everything corrected click **OK**(shown below)

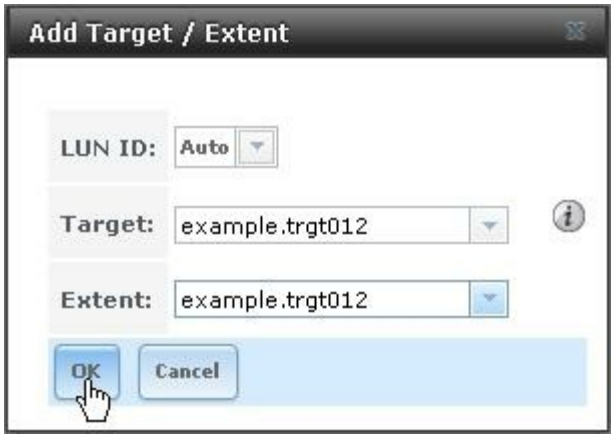


Finally, we can Associate the Target with the Extent!

To proceed: click **Add Target/Extent**

When the dialog appears simply select the **Target** and **Extent** to associate from the dropdowns. You can leave **LUN ID** set to **Auto**.

To proceed: click **OK**(shown below)



When the target has been successfully added to the system it will appear as shown below.

Congratulations!

Target Global Configuration | Portals | Initiators | Authorized Access | Targets | Extents | Associated Targets

Add Target / Extent

LUN ID	Target	Extent
	win7pro.trgt1	win7pro.trgt1
	torrentreaper.trgt013	torrentreaper.trgt013
	example.trgt012	example.trgt012

3.17-ZFS Snapshot Backups

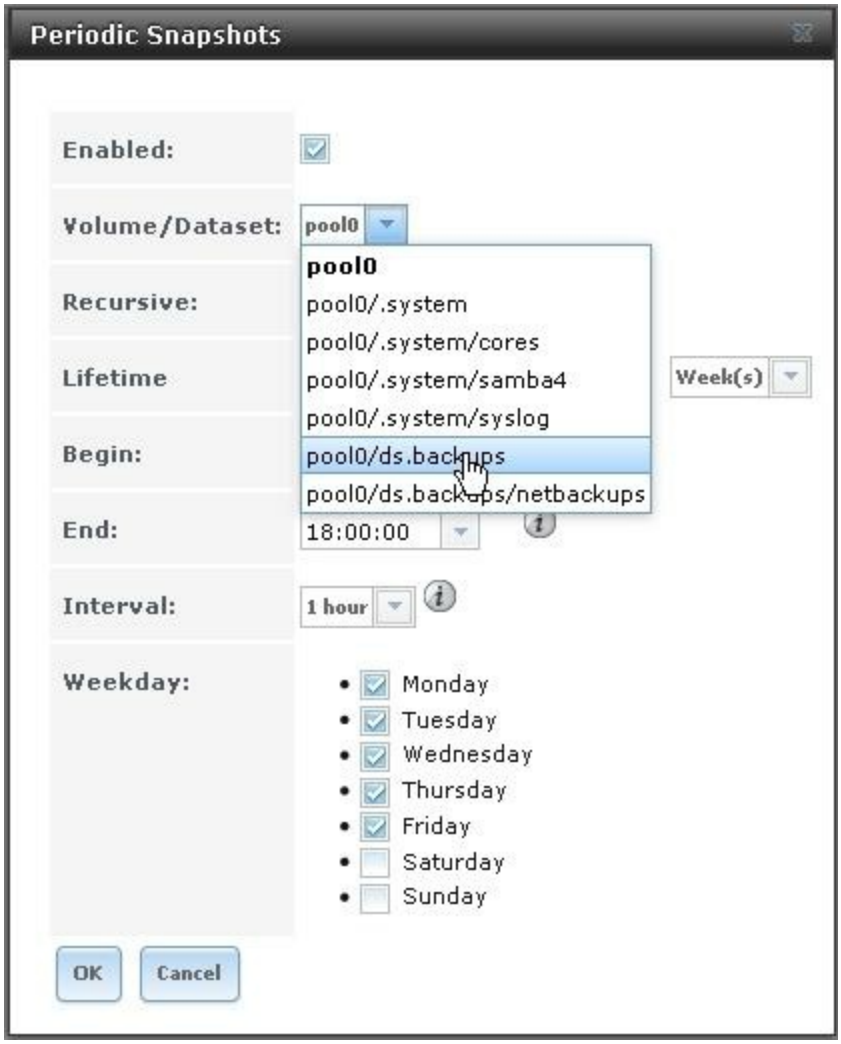
Probably, the **BEST** feature of the **ZFS** file system is ***copy on write***. This feature allows backups to be restored ***almost instantly*** from ***snapshot*** archives. When setup and used properly you will **NEVER** need another form of backup software... **EVER**!!! I **STRONGLY** suggest using my ***best practices method***. It involves running 2, 3, or 4 freeNAS servers all with the same datasets.

Any dataset hosting ***live data*** will be considered a **primary *dataset***. Each **primary *dataset*** will need to be manually **replicated** (once during setup) to all other freeNAS nodes. The ***primary datasets***(hosting live data) will be configured as ***Rsync push tasks*** on the node hosting the live shares. The ***backup datasets***(backup data only) will be configured as ***Rsync modules*** on any node **NOT** hosting live shares . With this method all datasets are replicated over every freeNAS node automatically.

ZFS snapshots can then be setup on each node using a different schedule. The **primary *datasets*** can be set to hourly or daily snapshots while the rest are set to weekly, monthly, etc. With enough storage overhead it is entirely possible to ***set it*** and ***forget it*** while it maintains backups for a ***year or more***. Let's setup a snapshot task now!

To proceed: click **Add Periodic Snapshot**(shown below)

For this snapshot task I am selecting the **ds.backups dataset**(pictured below).



Once again, the **Recursive** switch means that **ALL** nested datasets under **ds.backups** will be included in the snapshot. All other options should be self-explanatory(pictured below).

Periodic Snapshots

Enabled: ☑

Volume/Dataset: pool0/ds.backups

Recursive: ☑

Lifetime 2 Week(s)

Begin: 09:00:00

End: 18:00:00

Interval: 1 day

Weekday:
- ☑ Monday
- ☑ Tuesday
- ☑ Wednesday
- ☑ Thursday
- ☑ Friday
- ☐ Saturday
- ☐ Sunday

OK Cancel

Once saved, your snapshot task will appear in the list(pictured below).

Active Volumes ZFS Snapshots Periodic Snapshot Tasks ZFS Replication

Add Periodic Snapshot

Enabled	Volume/Dataset	When	Frequency
true	pool0/ds.backups	From 09:00:00 through 18:00:00, on every Monday, Tuesday, Wednesday, Thursday, Friday	every 1 day

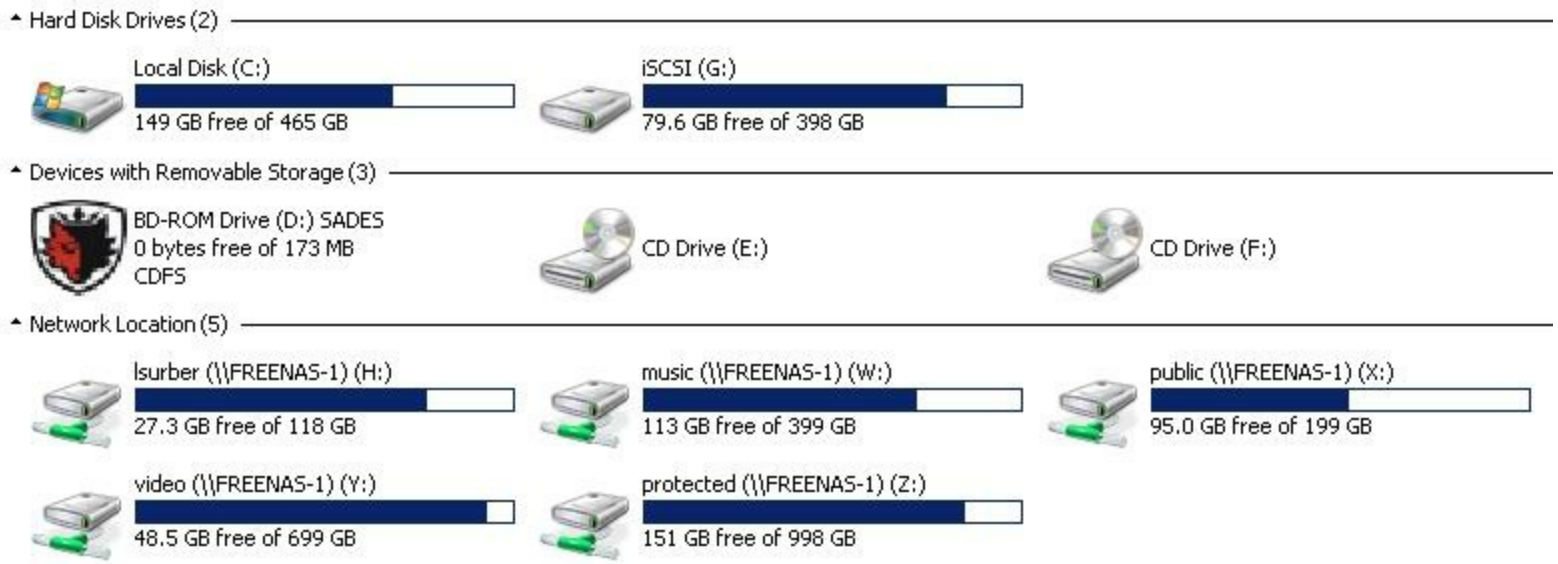
Notice that the new snapshot task was run almost immediately and can be accessed under the ZFS Snapshots tab(shown below). **At this point, users of Windows 7 or higher could now right click a CIFS file share on this dataset and mount or restore a file from the snapshot.**

Active Volumes | ZFS Snapshots | Periodic Snapshot Tasks | ZFS Replication

	Volume/Dataset	Snapshot Name	Used	Refer
...	No filter applied			
	pool0/ds.backups/netbackups	auto-20151214.0945-2w	0	144K
	pool0/ds.backups	auto-20151214.0945-2w	0	152K

3.18-Restore A Snapshot In Windows

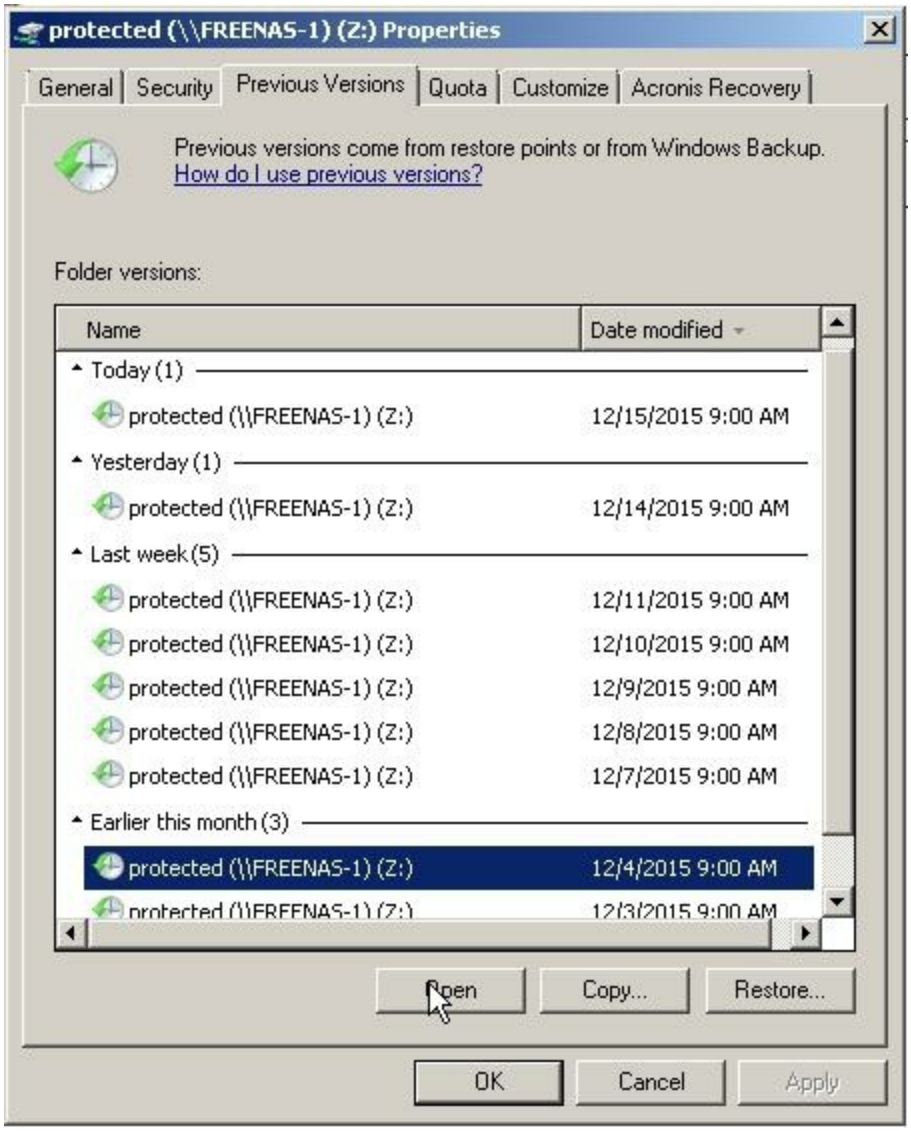
As an IT Administrator, it is very common to have end users calling on a daily basis saying they accidentally deleted their files. ZFS snapshots make this daily task easy to deal with on systems running Windows 7 or higher! Let's look at snapshot restore options on a Windows 7 machine(pictured below)!



Let's assume a user deleted a file from the mapped Z drive(shown above). To see available snapshots simply ***right click*** the drive then choose **Properties**(picture below).

When the dialog appears select the Previous Versions tab(pictured below). You will then have the

option to Open, Copy, or Restore any files over the range of snapshots in your schedule.



3.19-Rsync Replication

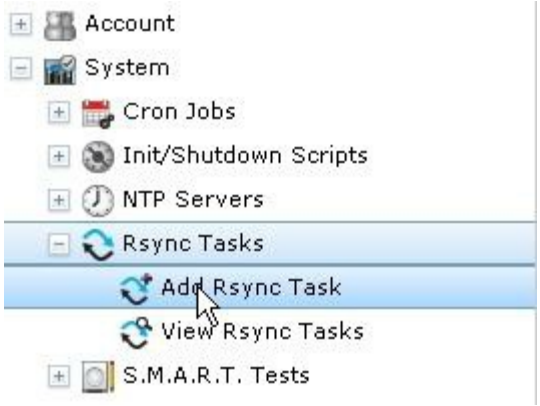
As mentioned previously, Rsync is a powerful backup utility widely used in the Linux community. It's poor man's High- Availability without a fence device! In many ways it's better! Of course, you won't have millisecond failover and true HA, but you will have several copies of data that can be accessed very quickly(5-10 minutes) if needed. The biggest BONUS here is price! A true hardware fenced High-Availability storage farm will cost you between $20000 and $100000 US Currency!

In order to setup Rsync for first run make sure you have ***created identical datasets on every freeNAS node***. So, if you have ***3 servers*** planned, then you will have ***3 sets of identical datasets*** for the Rsync backups. The ***primary datasets***(hosting live data) will be configured as ***Rsync push tasks*** on the node hosting the live shares. The ***backup datasets***(backup data only) will be configured as ***Rsync modules*** on any node **NOT** hosting live shares . With this method all datasets are replicated over every freeNAS node automatically.

3.19.1-Add The Rsync Push Task

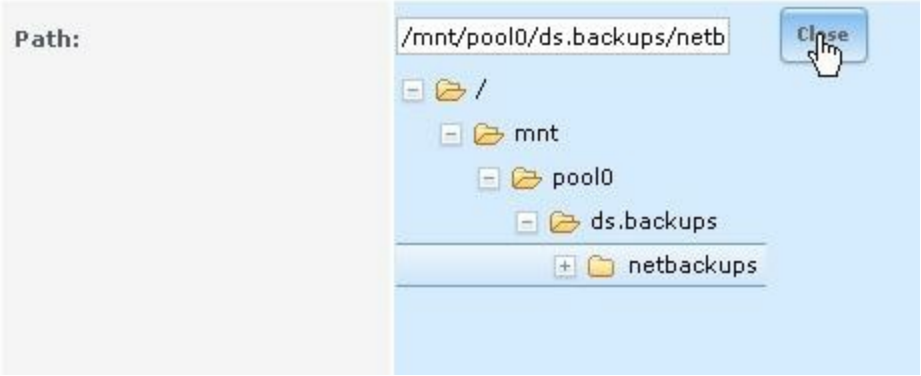
Let's add an Rsync task for the ***primary dataset*** named **netbackups**! This dataset contains important **live** data and is where Proxmox stores ALL of the ***VM image backups*** in a system configured like (Option-2) Optimized For Network Backed Storage!

To proceed: click **System>Rsync Tasks>Add Rsync Task**(shown below)



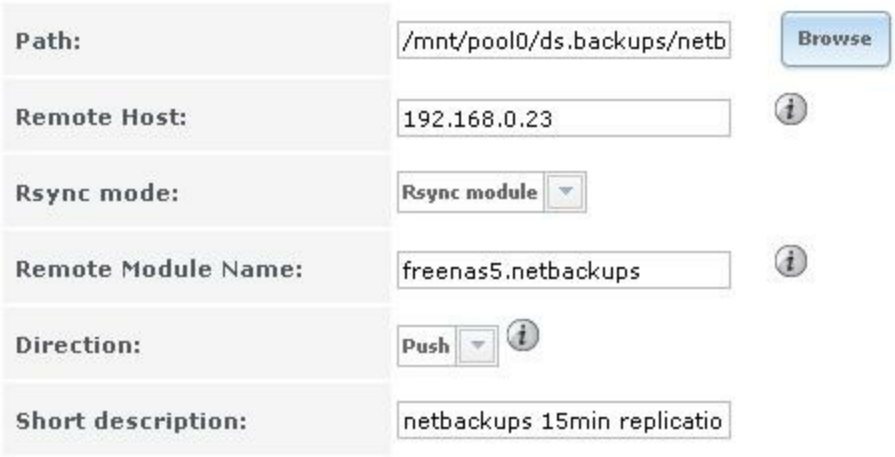
You should now see the task dialog box. Click **Browse** and select the appropriate dataset(as shown below).

Notice(below) that I have chosen the **netbackups** dataset which is ***nested*** under **ds.backups**! Please **NOTE** that when Rsync runs it will backup the entire **netbackups** dataset **folder.** This is **IMPORTANT** to remember when setting up the ***backup datasets*** on other nodes.



Next you will need to enter the **Remote Host** IP address and **Remote Module Name**. Notice, I have chosen **freenas5.netbackups** as the module name(pictured below). This identifies **freenas5** as the ***remote node*** and **netbackups** as the ***dataset folder*** I am backing up. Now, if I want to replicate **netbackups** to another server(freenas-2), the module names will ***uniquely identify each replication***.

Leave **Rsync mode** set to **module** and **Direction** set to **Push**. You may wish to enter a description that will indicate the frequency of the backups.



Next, select the desired **frequency** of the backup by adjusting the sliders(fig. 1-3 below). **NOTE**: Every 15 minutes may be ***too frequent*** for good ***performance***! This is just an example! I generally use 1 hour for files that change frequently and 1 day for static files.

fig. 1

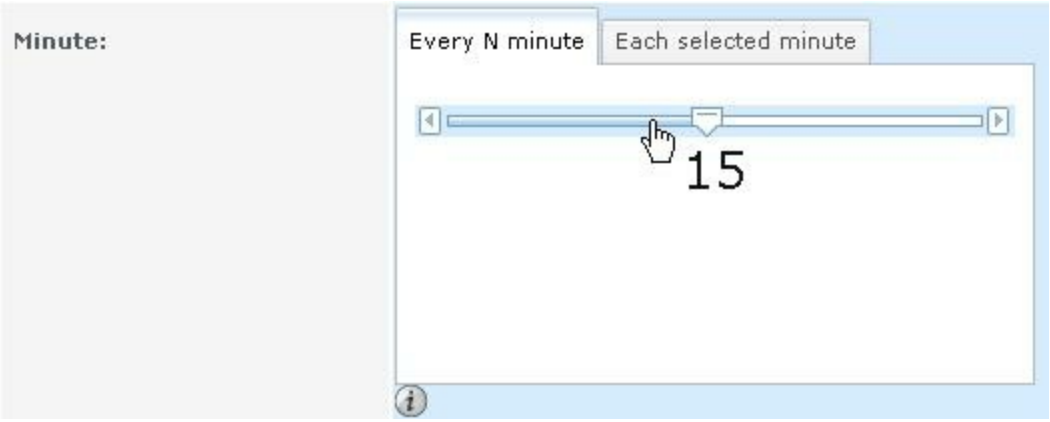
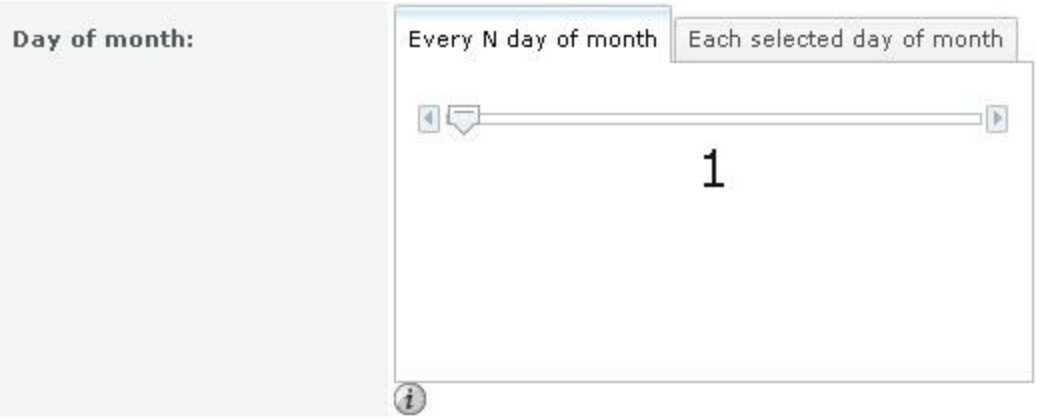
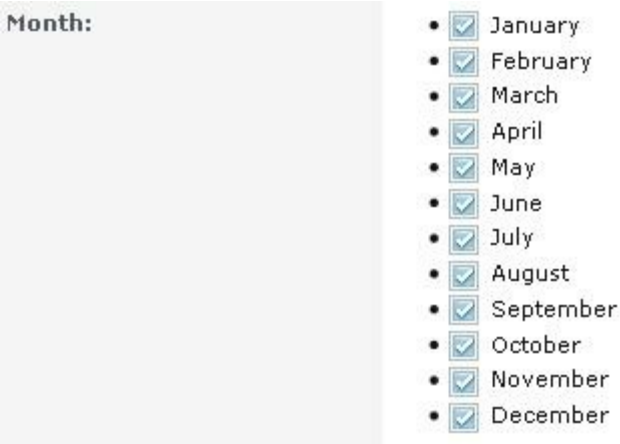


fig. 2

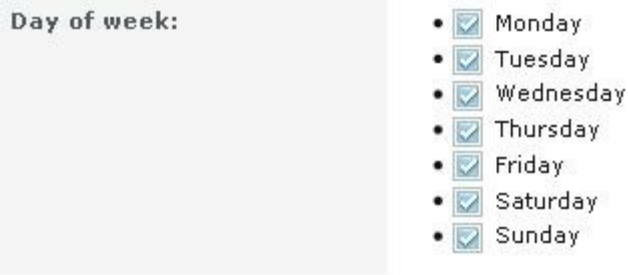
fig. 3



You may also choose a specific month(shown Below)



Or, choose a specific day of the week(shown below).



The default **User** is set to **root**(shown below). I would **NOT** change this unless you know what you're doing.

User: root

I like to use the options set as shown below.

Recursive:

Times:

Compress:

Archive:

Delete:

Quiet:

Preserve permissions:

Preserve extended attributes:

Extra options:

Enabled:

The screenshot below shows what a working Rsync Tasks table looks like. These tasks are configured on a fileserver named freeNAS-1 hosting live data. All datasets are pushed to Remote Modules on nodes freeNAS-2 and freeNAS-4 every hour.

Add Rsync Task

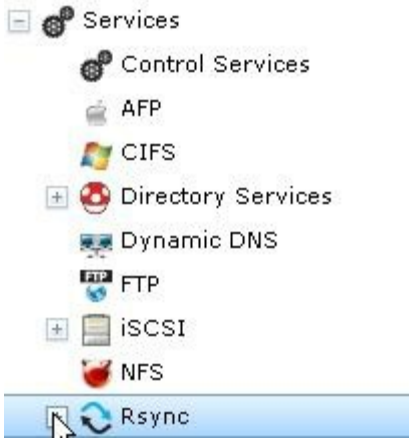
Path	Remote Host	Remote SSH Port	Remote Module Name	Remote Path	Direction	Minute	Hour	Day of month	Month	Day of week
/mnt/pool0/ds.backups/websites	192.168.0.11	22	freenas-2.websites		push	00	Every hour	Everyday	Every month	Everyday
/mnt/pool0/ds.backups/websites	192.168.0.22	22	freenas-4.websites		push	00	Every hour	Everyday	Every month	Everyday
/mnt/pool0/ds.backups/win7pro	192.168.0.11	22	freenas-2.win7pro		push	00	Every hour	Everyday	Every month	Everyday
/mnt/pool0/ds.backups/win7pro	192.168.0.22	22	freenas-4.win7pro		push	00	Every hour	Everyday	Every month	Everyday
/mnt/pool0/ds.filestore/protected	192.168.0.11	22	freenas-2.protected		push	00	Every hour	Everyday	Every month	Everyday
/mnt/pool0/ds.filestore/protected	192.168.0.22	22	freenas-4.protected		push	00	Every hour	Everyday	Every month	Everyday
/mnt/pool0/ds.filestore/public	192.168.0.11	22	freenas-2.public		push	00	Every hour	Everyday	Every month	Everyday
/mnt/pool0/ds.filestore/public	192.168.0.22	22	freenas-4.public		push	00	Every hour	Everyday	Every month	Everyday
/mnt/pool0/ds.home/administrator	192.168.0.11	22	freenas-2.administrator		push	00	Every hour	Everyday	Every month	Everyday
/mnt/pool0/ds.home/administrator	192.168.0.22	22	freenas-4.administrator		push	00	Every hour	Everyday	Every month	Everyday
/mnt/pool0/ds.home/dbrewer	192.168.0.11	22	freenas-2.dbrewer		push	00	Every hour	Everyday	Every month	Everyday
/mnt/pool0/ds.home/dbrewer	192.168.0.22	22	freenas-4.dbrewer		push	00	Every hour	Everyday	Every month	Everyday
/mnt/pool0/ds.home/lsurber	192.168.0.11	22	freenas-2.lsurber		push	00	Every hour	Everyday	Every month	Everyday
/mnt/pool0/ds.home/lsurber	192.168.0.22	22	freenas-4.lsurber		push	00	Every hour	Everyday	Every month	Everyday
/mnt/pool0/ds.mediaserver/music	192.168.0.11	22	freenas-2.music		push	00	Every hour	Everyday	Every month	Everyday
/mnt/pool0/ds.mediaserver/music	192.168.0.22	22	freenas-4.music		push	00	Every hour	Everyday	Every month	Everyday
/mnt/pool0/ds.mediaserver/video	192.168.0.11	22	freenas-2.video		push	00	Every hour	Everyday	Every month	Everyday
/mnt/pool0/ds.mediaserver/video	192.168.0.22	22	freenas-4.video		push	00	Every hour	Everyday	Every month	Everyday
/mnt/pool0/ds.proxmox/nfs.containers	192.168.0.11	22	freenas-2.nfs.containers		push	00	Every hour	Everyday	Every month	Everyday
/mnt/pool0/ds.proxmox/nfs.containers	192.168.0.22	22	freenas-4.nfs.containers		push	00	Every hour	Everyday	Every month	Everyday
/mnt/pool0/ds.proxmox/nfs.images	192.168.0.11	22	freenas-2.nfs.images		push	00	Every hour	Everyday	Every month	Everyday
/mnt/pool0/ds.proxmox/nfs.images	192.168.0.22	22	freenas-4.nfs.images		push	00	Every hour	Everyday	Every month	Everyday
/mnt/pool0/ds.proxmox/nfs.isostore	192.168.0.11	22	freenas-2.nfs.isostore		push	00	Every hour	Everyday	Every month	Everyday
/mnt/pool0/ds.proxmox/nfs.isostore	192.168.0.22	22	freenas-4.nfs.isostore		push	00	Every hour	Everyday	Every month	Everyday
/mnt/pool0/ds.proxmox/nfs.netbackups	192.168.0.11	22	freenas-2.nfs.netbackups		push	00	Every hour	Everyday	Every month	Everyday
/mnt/pool0/ds.proxmox/nfs.netbackups	192.168.0.22	22	freenas-4.nfs.netbackups		push	00	Every hour	Everyday	Every month	Everyday
/mnt/pool0/ds.proxmox/nfs.templates	192.168.0.11	22	freenas-2.nfs.templates		push	00	Every hour	Everyday	Every month	Everyday
/mnt/pool0/ds.proxmox/nfs.templates	192.168.0.22	22	freenas-4.nfs.templates		push	00	Every hour	Everyday	Every month	Everyday

Edit Delete

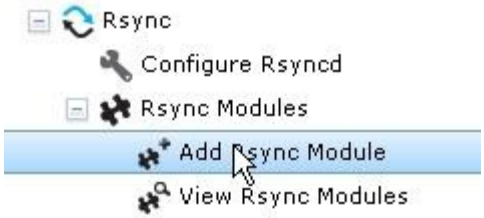
3.19.2-Add The Rsync Module

Let's setup an **Rsync Module** for a backup dataset on one of the other freeNAS nodes to synchronize the **netbackups** dataset now!

To proceed: click **Services>Rsync** (shown below)



Now, click **Add Rync Module**(shown below)



You should now see the module dialog box(pictured below). Enter the **Module name** from the ***Rsync push task*** you previously configured(**freenas5.netbackups**). You may wish to use the same **Comment** from the ***Rsync push task***. Leave the **Access Mode** set to Read/Write and **User** set to ***root.***

NOTICE: I have added the IP address of the ***primary*** freeNAS ***push task node*** in the **Hosts allow** field to limit access.

MOST IMPORTANT: It is critical the **Path** be set to /mnt/pool0/**ds.backups** and **NOT** /mnt/pool0/**ds.backups/netbackups** or you will end up with a ***nested copy*** that looks something like this /mnt/pool0/ds.backups/netbackups/netbackups.

Edit

Module name:	freenas5.netbackups
Comment:	netbackups 15min replicatio
Path:	/mnt/pool0/ds.backups Browse
Access Mode:	Read and Write
Maximum connections:	0
User:	root
Group:	wheel
Hosts allow:	192.168.0.22
Hosts deny:	
Auxiliary parameters:	

OK Cancel Delete

The screenshot below shows what a working Rsync Modules table looks like. These Modules are configured on a machine named freeNAS-4. All datasets are pushed from freeNAS-1 every hour.

Add Rsync Module

Module name	Comment	Path	Access Mode	Maximum connections	User	Group	Hosts allow
freenas-4.administrator		/mnt/pool0/ds.home	rw	0	root	wheel	192.168.0.10
freenas-4.dbrewer		/mnt/pool0/ds.home	rw	0	root	wheel	192.168.0.10
freenas-4.lsurber		/mnt/pool0/ds.home	rw	0	root	wheel	192.168.0.10
freenas-4.music		/mnt/pool0/ds.mediaserver	rw	0	root	wheel	192.168.0.10
freenas-4.nfs.containers		/mnt/pool0/ds.proxmox	rw	0	root	wheel	192.168.0.10
freenas-4.nfs.images		/mnt/pool0/ds.proxmox	rw	0	root	wheel	192.168.0.10
freenas-4.nfs.isostore		/mnt/pool0/ds.proxmox	rw	0	root	wheel	192.168.0.10
freenas-4.nfs.netbackups		/mnt/pool0/ds.proxmox	rw	0	root	wheel	192.168.0.10
freenas-4.nfs.netbackups2		/mnt/pool0/ds.proxmox	rw	0	root	wheel	192.168.0.11
freenas-4.nfs.templates		/mnt/pool0/ds.proxmox	rw	0	root	wheel	192.168.0.10
freenas-4.protected		/mnt/pool0/ds.filestore	rw	0	root	wheel	192.168.0.10
freenas-4.public		/mnt/pool0/ds.filestore	rw	0	root	wheel	192.168.0.10
freenas-4.video		/mnt/pool0/ds.mediaserver	rw	0	root	wheel	192.168.0.10
freenas-4.websites		/mnt/pool0/ds.backups	rw	0	root	wheel	192.168.0.10
freenas-4.win7pro		/mnt/pool0/ds.backups	rw	0	root	wheel	192.168.0.10

3.19.3-Tips On Using Rsync

Setting up Tasks and Modules can be confusing at first so be patient and think about what you're doing.

- Remember that when configuring **Rsync** in ***Push mode***(used in this book) ***live datasets*** will have a **Task** and ***backup datasets*** will have a **Module**.
- Avoid having live datasets on every freeNAS node. You should have at least 1 freeNAS node where NO live data is hosted. This *normally* means there will be NO Rsync Push Tasks on that machine.
- Double check every Task and Module you create. This will help prevent ***overwriting*** important live data.
- When setting up a new freeNAS server with a large amount of data only add a few modules at a time. You would experience a big performance hit if several Terabytes of data tried to synchronize all at once.
- Use good naming practices to avoid confusion.
- Use dedicated network adapters and an isolated subnet to dramatically improve performance. You may also want to limit adapter throughput OR use 100 Base virtual adapters for these dedicated links.

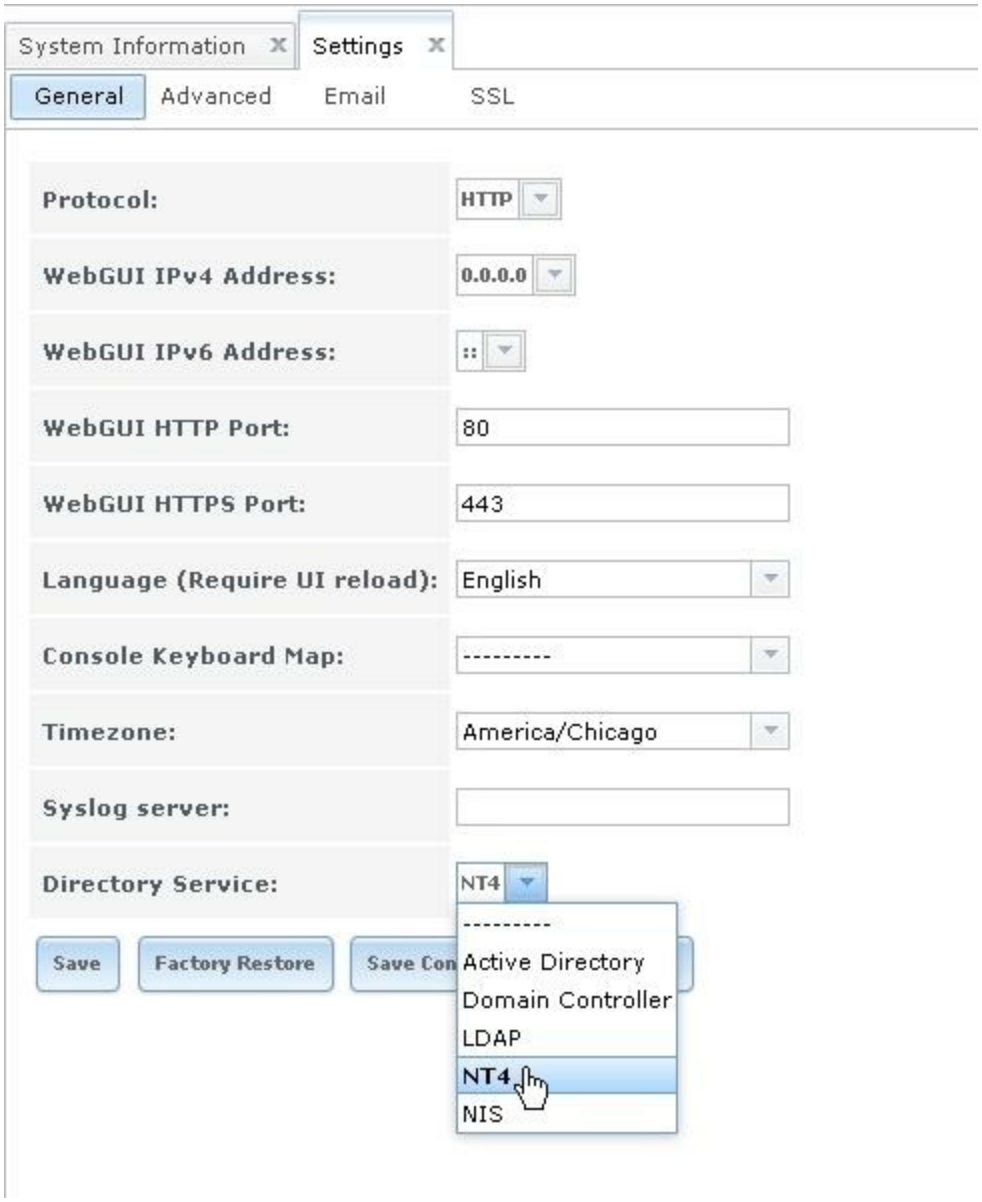
3.20-Domain Membership

A domain directory consists of a ***central database*** and allows **MUCH** easier **management** of Users, Groups, and Network Services. Most domains are managed by Microsoft **active directory** running on a Windows server. In this book I have included an ***open source alternative*** which leverages the powerful **Samba4** platform running on **Zentyal** Small Business Server.

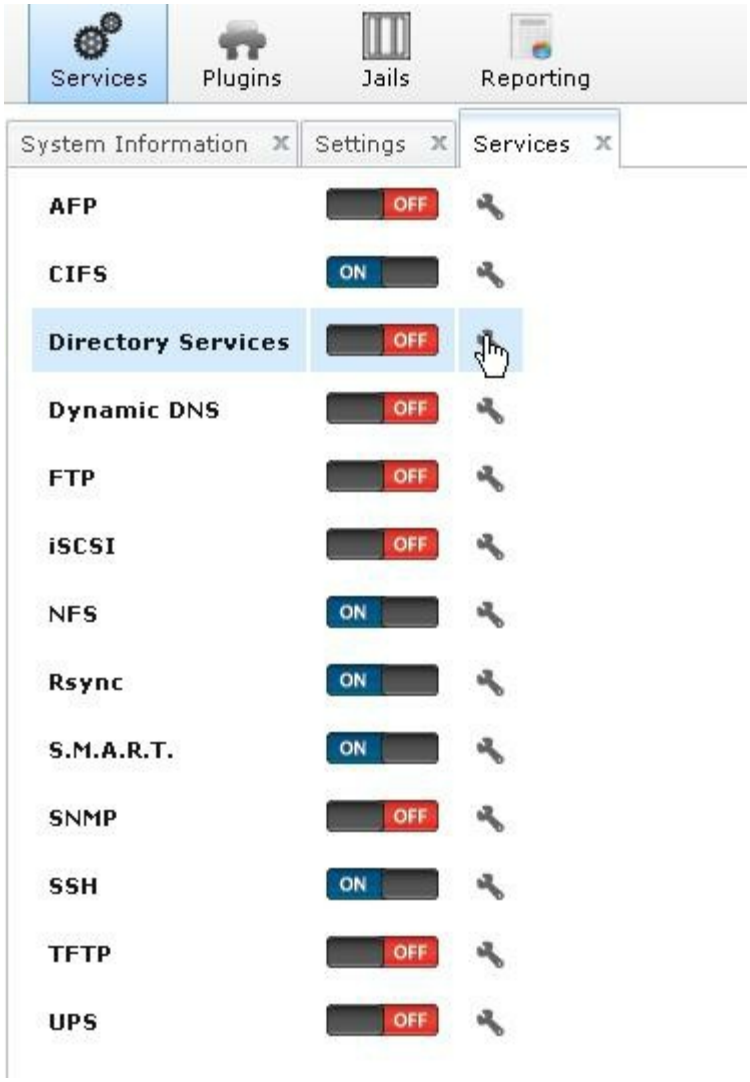
Although freeNAS is capable of acting as a Domain Controller, I prefer to use **Zentyal** because it keeps things ***modular*** and it can be readily setup for ***Master/Slave*** control. This method is preferred because it adds ***redundancy*** to the ***central database***!

Let's add this freeNAS server to a Zentyal controlled domain. In the tradition of ***keeping things simple*** and ***compatible*** I will use the older **NT4** database style(shown below).

To configure Domain Directory Service click **System>General** then select **NT4** from the dropdown list(shown below). Don't forget to save the setting!



Next, go to **Services>Directory Services** and click the **wrench icon**(pictured below)



You should now see the **Directory Service** dialog(shown below). Enter the Domain Controller ***IP address*** instead of the host name. This is the address of the **Zentyal** server. **NOTE**: This address should also be entered in your ***pfSense DHCP static reservation list***.

PAY ATTENTION HERE: With the **NT4** based directory you **DO NOT** need to enter **.com**, **.org**, **.us**, etc domain suffixes. Also, your **Workgroup Name** is limited to ***15 characters***. I have entered **YOURWEBS** in the **Workgroup Name** even though the domain name I will be controlling is **YOURWEBS.US**(pictured below).

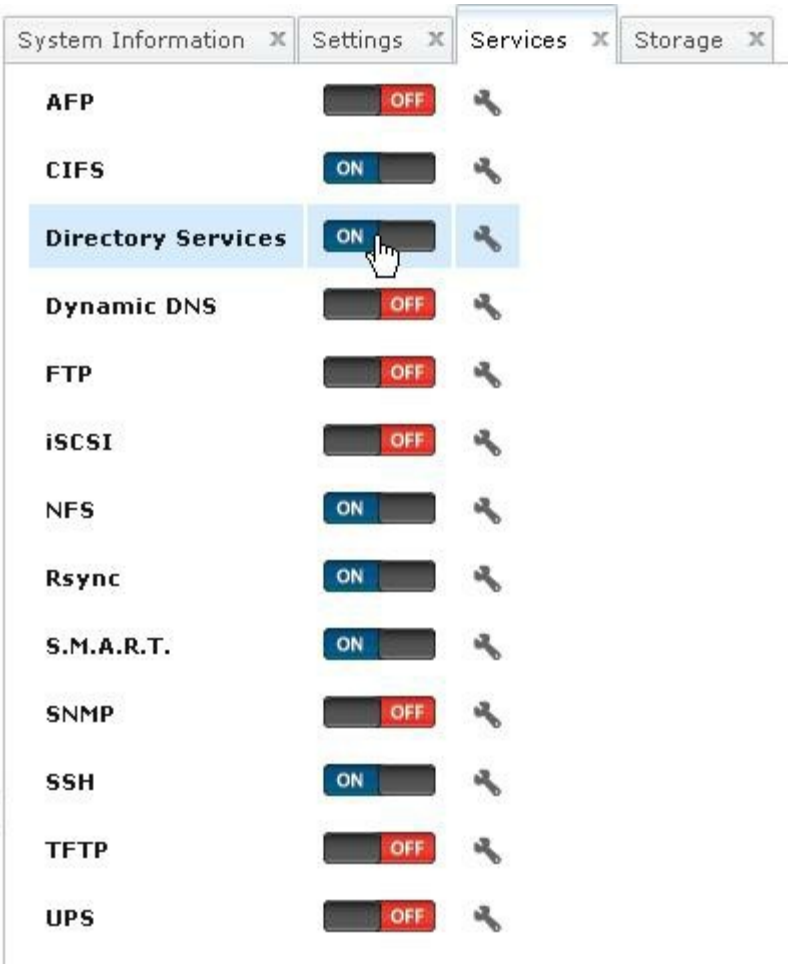
Earlier we setup **CIFS**(Windows) shares on your new freeNAS server. When configuring the machine for domain membership the CIFS Workgroup settings should match those for Directory Services.

Double check your settings now by going to **Services>CIFS** then clicking the **wrench icon.** I have included my settings for your reference(pictured below). Remember to save your changes!

CIFS Settings

NetBIOS name:	freenas-4
Workgroup:	YOURWEBS
Description:	FreeNAS Server
DOS charset:	CP437
UNIX charset:	UTF-8
Log level:	Minimum
Use syslog:	☐
Local Master:	☑
Time Server for Domain:	☑
Guest account:	nobody
File mask:	
Directory mask:	
EA Support:	☐
Support DOS File Attributes:	☑
Allow Empty Password:	☐
Auxiliary parameters:	

Now you can enable the Directory Service by clicking on the switch as shown below. It should turn blue when enabled.



The final step is to **Rebuild the cache**. Go to **System>Settings>Advanced** then click **Rebuild LDAP/AD Cache** at the bottom of the page(shown below). **NOTE**: sometimes it is necessary to reboot the server for all changes to become active.

System Information | Settings | Services

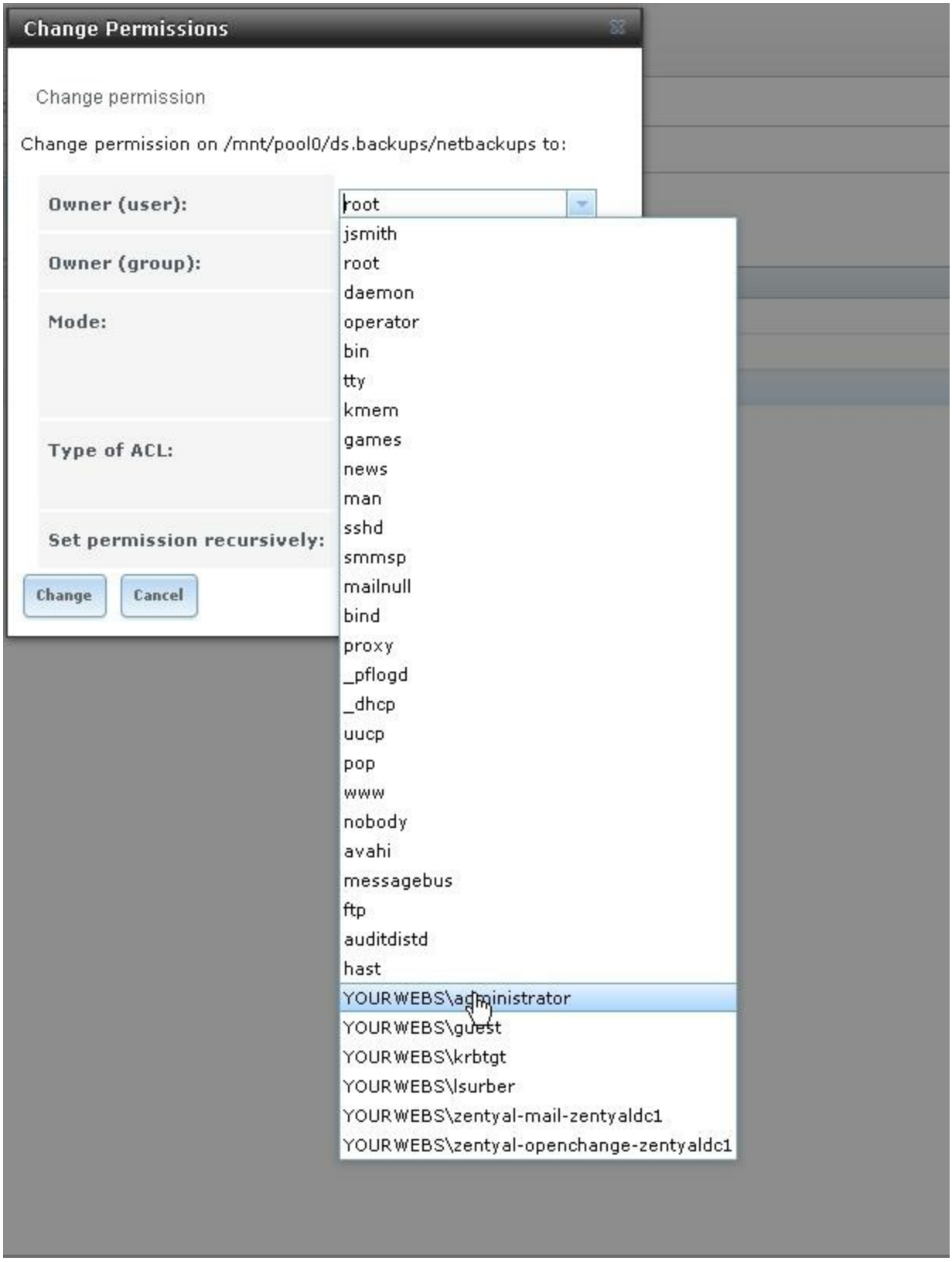
General | Advanced | Email | SSL

Enable Console Menu:	☑
Use Serial Console:	☐
Serial Port Address:	0x2f8
Serial Port Speed:	9600
Enable screen saver:	☐
Enable powerd (Power Saving Daemon):	☐
Swap size on each drive in GiB, affects new disks only. Setting this to 0 disables swap creation completely (STRONGLY DISCOURAGED).	2
Show console messages in the footer:	☐
Show tracebacks in case of fatal errors:	☑
Show advanced fields by default:	☑
Enable autotune:	☐
Enable debug kernel:	☐
Enable automatic upload of kernel crash dumps:	☑
MOTD banner:	Welcome to FreeNAS
System dataset pool:	pool0
Use system dataset for syslog:	☑

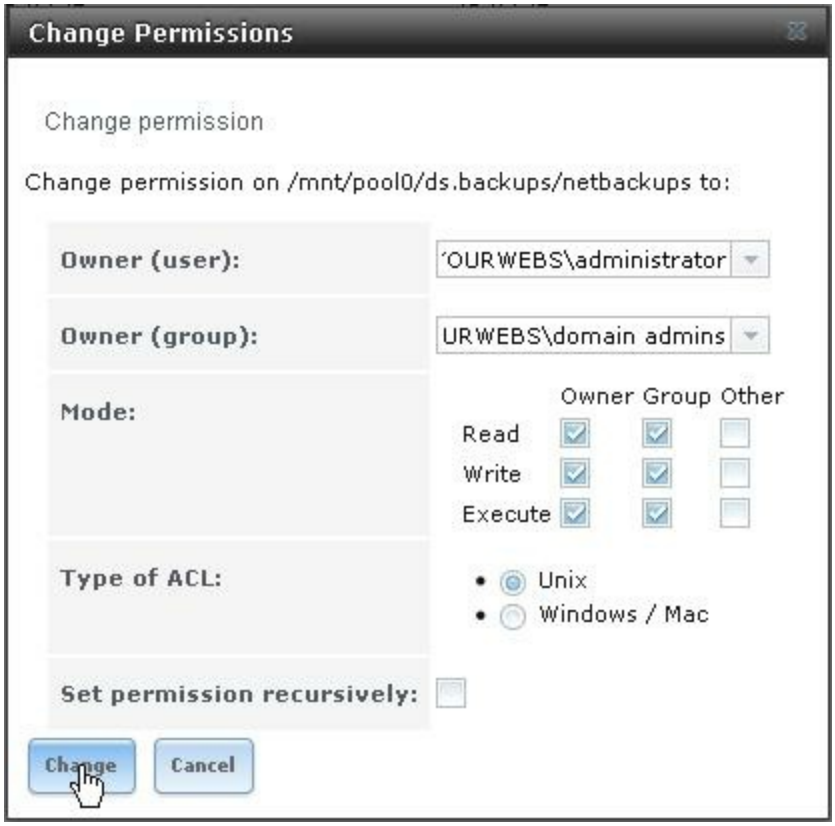
Save | Rebuild LDAP/AD Cache | Save Debug | Firmware Update

3.20.1-Domain Permissions

With the server now being an active ***domain member*** you should now see ***additional*** Users and Groups in your dataset Permissions dialog. To demonstrate this I have included the permissions dialog for the **netbackups** dataset we created earlier. Notice the ***additional*** Users at the ***bottom*** of the dropdown list(pictured below).



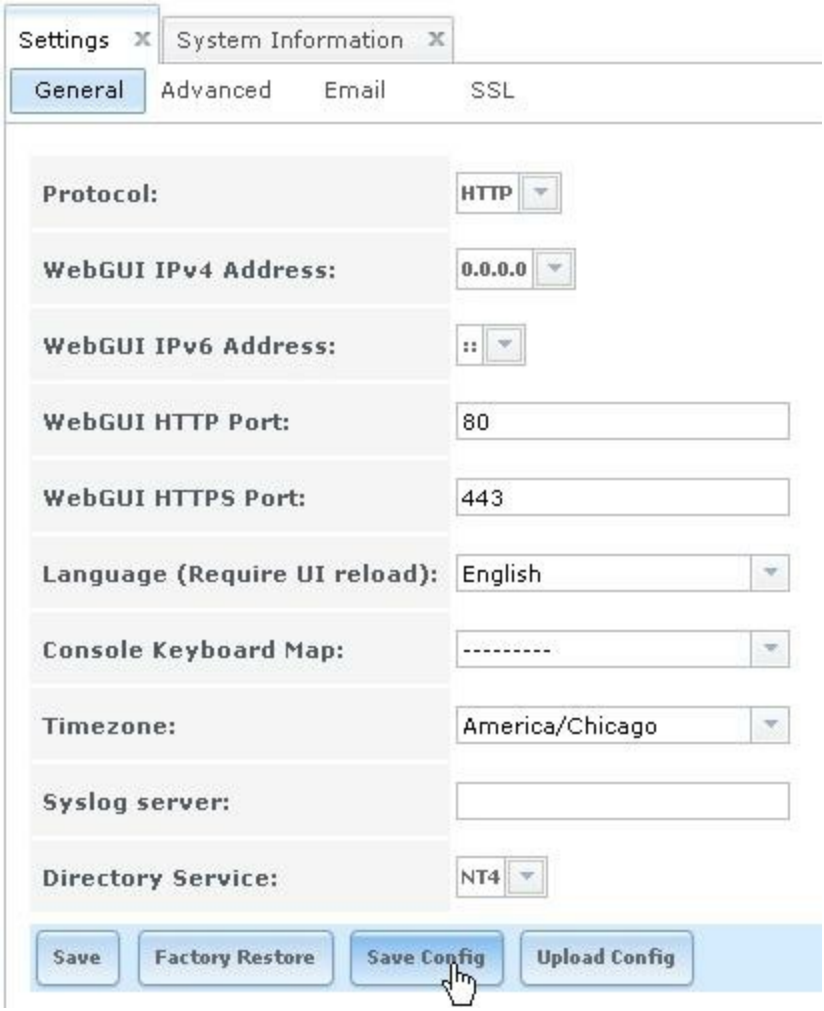
As an example I have changed the owner permissions on the **netbackups** dataset(pictured below). With these new permissions, **ONLY** domain administrators would have access to the dataset.


Change Permissions
Change permission
Change permission on /mnt/pool0/ds.backups/netbackups to:
Owner (user):
OURWEBS\administrator
Owner (group):
URWEBS\domain admins
Mode:
Owner Group Other
Read
Write
Execute
Type of ACL:
Unix
Windows / Mac
Set permission recursively:
Change
Cancel

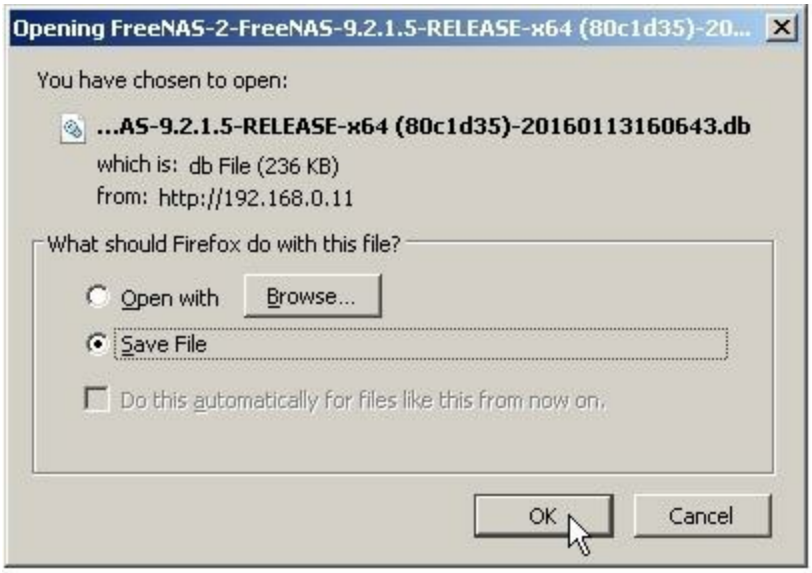
3.21-Configuration Backups

Besides using VM image backups it is also wise to keep a copy of the freeNAS configuration. The configuration backup is especially important when developers rewrite the build in a way that breaks certain packages on update. In these instances your VM image backup will only get you back to the version you were using. I have NOT had this happen with freeNAS, so don't worry too much!

To access the configuration backup page: click **System>Settings>General** followed by **Save Config**(pictured below).



Save the configuration file to disk when the download dialog appears(shown below). **HINT**: I recommend keeping a copy of this on thumb drive!



Restoring your freeNAS configuration should be self-explanatory! Simply use the **Upload Config** option instead!

Book 4: Zentyal Domain Controller

4.1-Introduction To Zentyal

Zentyal started in 2004 as an Open Source project. It has a very loyal global community and is actively developed. Zentyal Small Business Server CE is actually a fully fledged business solution. The latest versions leverage the powerful Samba 4 package which effectively emulates a Microsoft Domain Controller. It comes as a complete standalone distribution in CD\DVD ISO format which makes installation a breeze! This makes Zentyal a no brainer for inclusion as a modular building block in our 4 in 1 system.

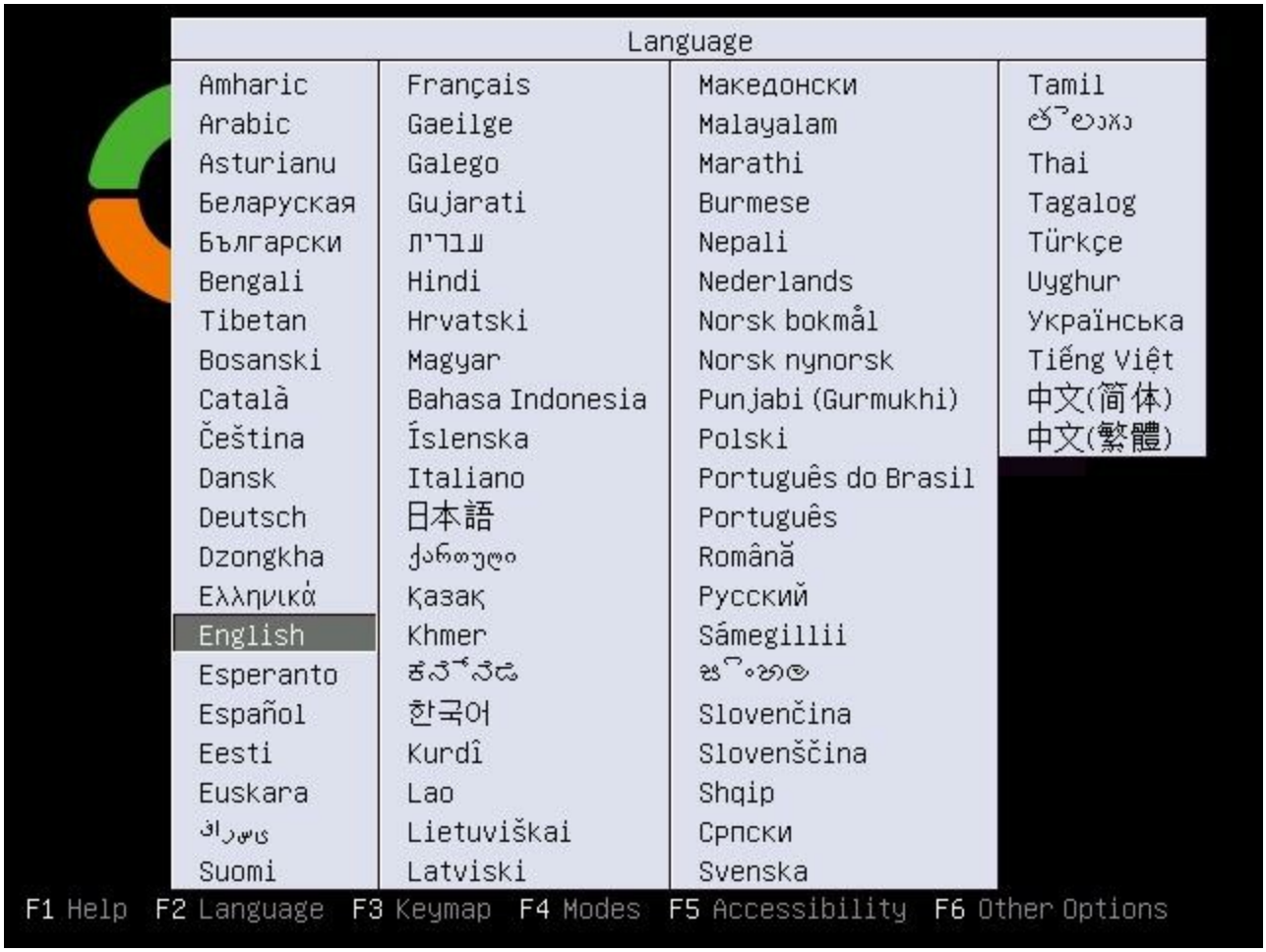
In our system we will use it as an Active Directory Domain Controller. In this book I am using the Zentyal 4.0 64 bit version. You can download this exact version at Sourceforge here: zentyal-4.0-amd64.iso NOTE: The latest version is now called Zentyal Server Development Edition. The interface remains largely the same but I would still recommend matching the version I have use to avoid any issues. If you are comfortable with the latest version it can be downloaded directly from the Zentyal home page here: Zentyal Server Development Edition

4.2-Installing Zentyal

The installation process for Zentyal is similar to most other operating systems. Before installation can begin you must ***create the VM configuration***. I recommend a ***12Gb IDE virtual disk*** with ***8Gb of Ram*** for this install. If you need to review those steps again click here: 1.9-Creating VM Configuration. You may also want to add a DHCP client reservation in pfSense before you begin the actual install.

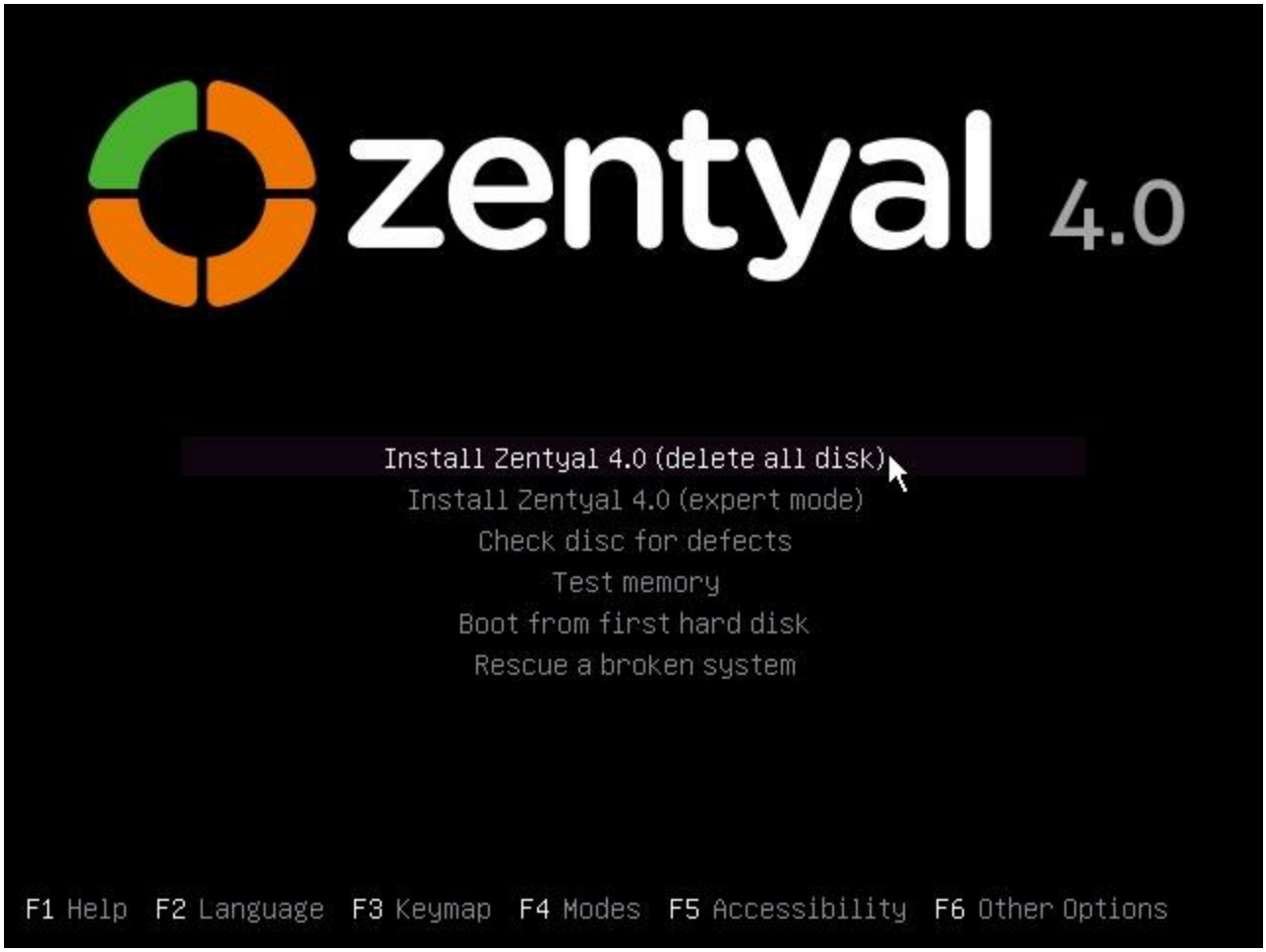
Once the machine is started you will see the language selection screen(pictured below).

To proceed: press **ENTER**



Next, you will see the mode selection screen(shown below).

To proceed: press **ENTER**



The default language is set to English(pictured below). Notice: the navigation map for moving, selecting, and activating is located at the bottom of the screen.

To proceed: press **ENTER**

[!!] Select a language

Choose the language to be used for the installation process. The selected language will also be the default language for the installed system.

Language:

C	-	No localization
Albanian	-	Shqip
Arabic	-	عربي
Asturian	-	Asturianu
Basque	-	Euskara
Belarusian	-	Беларуская
Bosnian	-	Bosanski
Bulgarian	-	български
Catalan	-	Català
Chinese (Simplified)	-	中文(简体)
Chinese (Traditional)	-	中文(繁體)
Croatian	-	Hrvatski
Czech	-	Čeština
Danish	-	Dansk
Dutch	-	Nederlands
English	-	English
Esperanto	-	Esperanto
Estonian	-	Eesti
Finnish	-	Suomi
French	-	Français
Galician	-	Galego
German	-	Deutsch
Greek	-	Ελληνικά

<Go Back>

<Tab> moves; <Space> selects; <Enter> activates buttons

Now, select your location(pictured below).

To proceed: press **ENTER**

```
[!!] Select your location

The selected location will be used to set your time zone and also for example to help
select the system locale. Normally this should be the country where you live.

This is a shortlist of locations based on the language you selected. Choose "other" if
your location is not listed.

Country, territory or area:

                                    Antigua and Barbuda
                                    Australia
                                    Botswana
                                    Canada
                                    Hong Kong
                                    India
                                    Ireland
                                    New Zealand
                                    Nigeria
                                    Philippines
                                    Singapore
                                    South Africa
                                    United Kingdom
                                    United States
                                    Zambia
                                    Zimbabwe
                                    other

    <Go Back>

<Tab> moves; <Space> selects; <Enter> activates buttons
```

Optionally, you may choose to detect your keyboard layout(shown below). We will not auto-detect our keyboard.

To proceed: select **No** then press **ENTER**

[!] Configure the keyboard

You can try to have your keyboard layout detected by pressing a series of keys. If you do not want to do this, you will be able to select your keyboard layout from a list.

Detect keyboard layout?

<Go Back> <Yes> <No>

<Tab> moves; <Space> selects; <Enter> activates buttons

Next, select the country of origin for your keyboard(pictured below).

To proceed: press **ENTER**

```
[!] Configure the keyboard

The layout of keyboards varies per country, with some countries having multiple common
layouts. Please select the country of origin for the keyboard of this computer.

Country of origin for the keyboard:

                    Armenian
                    Azerbaijani
                    Bambara
                    Bangla
                    Belarusian
                    Belgian
                    Bosnian
                    Braille
                    Bulgarian
                    Burmese
                    Chinese
                    Croatian
                    Czech
                    Danish
                    Dhivehi
                    Dutch
                    Dzongkha
                    English (Cameroon)
                    English (Ghana)
                    English (Nigeria)
                    English (South Africa)
                    English (UK)
                    English (US)

    <Go Back>

<Tab> moves; <Space> selects; <Enter> activates buttons
```

Now, select the proper layout for your keyboard(shown below).

To proceed: press **ENTER**

```
[!] Configure the keyboard

Please select the layout matching the keyboard for this machine.

Keyboard layout:

 English (US)
 English (US) - Cherokee
 English (US) - English (Colemak)
 English (US) - English (Dvorak alternative international no dead keys)
 English (US) - English (Dvorak)
 English (US) - English (Dvorak, international with dead keys)
 English (US) - English (Macintosh)
 English (US) - English (US, alternative international)
 English (US) - English (US, international with dead keys)
 English (US) - English (US, with euro on 5)
 English (US) - English (Workman)
 English (US) - English (Workman, international with dead keys)
 English (US) - English (classic Dvorak)
 English (US) - English (international AltGr dead keys)
 English (US) - English (left handed Dvorak)
 English (US) - English (programmer Dvorak)
 English (US) - English (right handed Dvorak)
 English (US) - English (the divide/multiply keys toggle the layout)
 English (US) - Russian (US, phonetic)
 English (US) - Serbo-Croatian (US)

    <Go Back>

<Tab> moves; <Space> selects; <Enter> activates buttons
```

Now, you will be prompted to set a hostname. If you already assigned a static DHCP reservation your hostname should appear(pictured below).

To proceed: Select **Continue** then press **<u>ENTER</u>**

[!] Configure the network

Please enter the hostname for this system.

The hostname is a single word that identifies your system to the network. If you don't know what your hostname should be, consult your network administrator. If you are setting up your own home network, you can make something up here.

Hostname:

Zentyal DC2

<Go Back> <Continue>

<Tab> moves; <Space> selects; <Enter> activates buttons

Next, choose a username for account administration(shown below).

To proceed: Select **Continue** then press **ENTER**

[!!] Set up users and passwords

Select a username for the new account. Your first name is a reasonable choice. The username should start with a lower-case letter, which can be followed by any combination of numbers and more lower-case letters.

Username for your account:

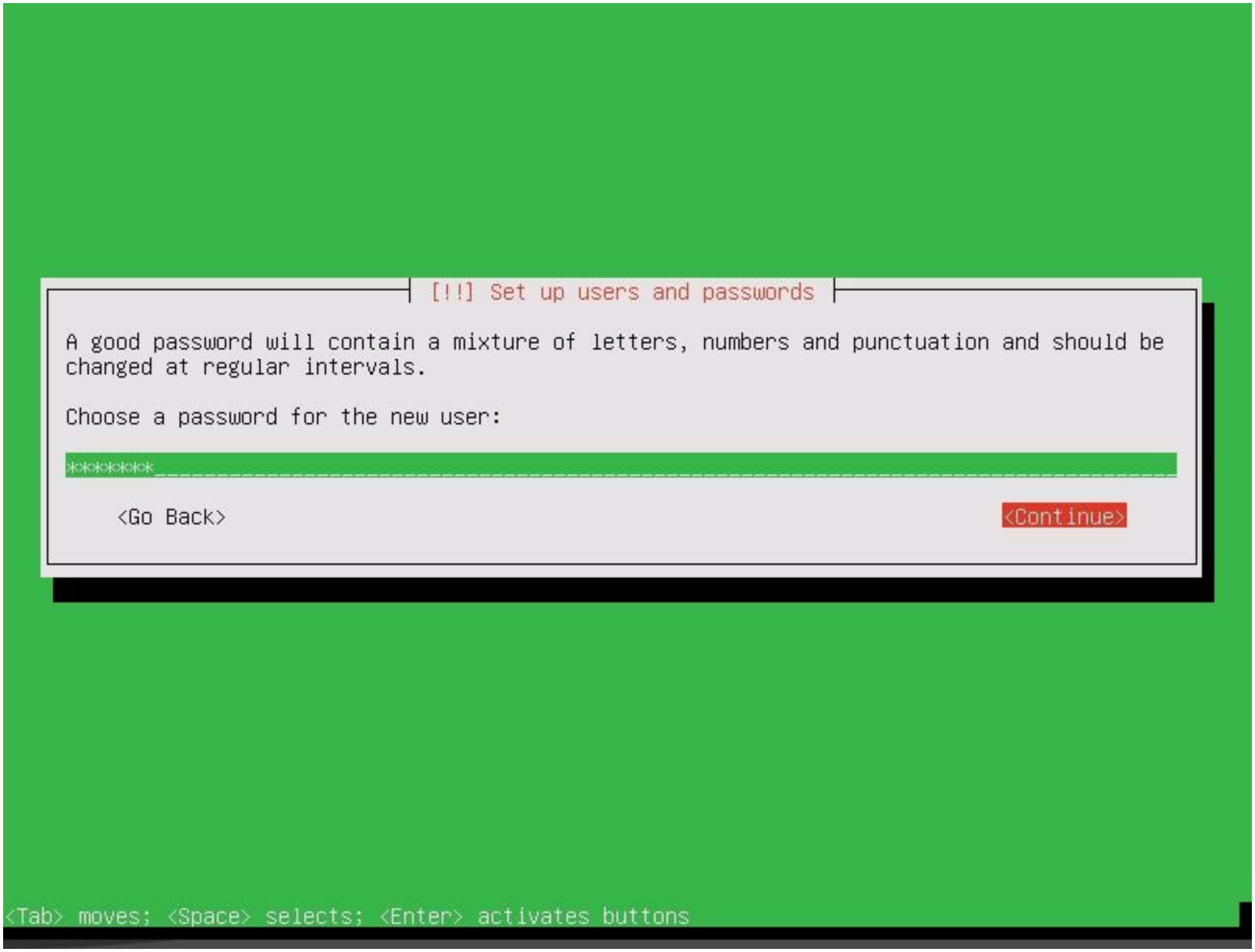
zentyal

<Go Back> <Continue>

<Tab> moves; <Space> selects; <Enter> activates buttons

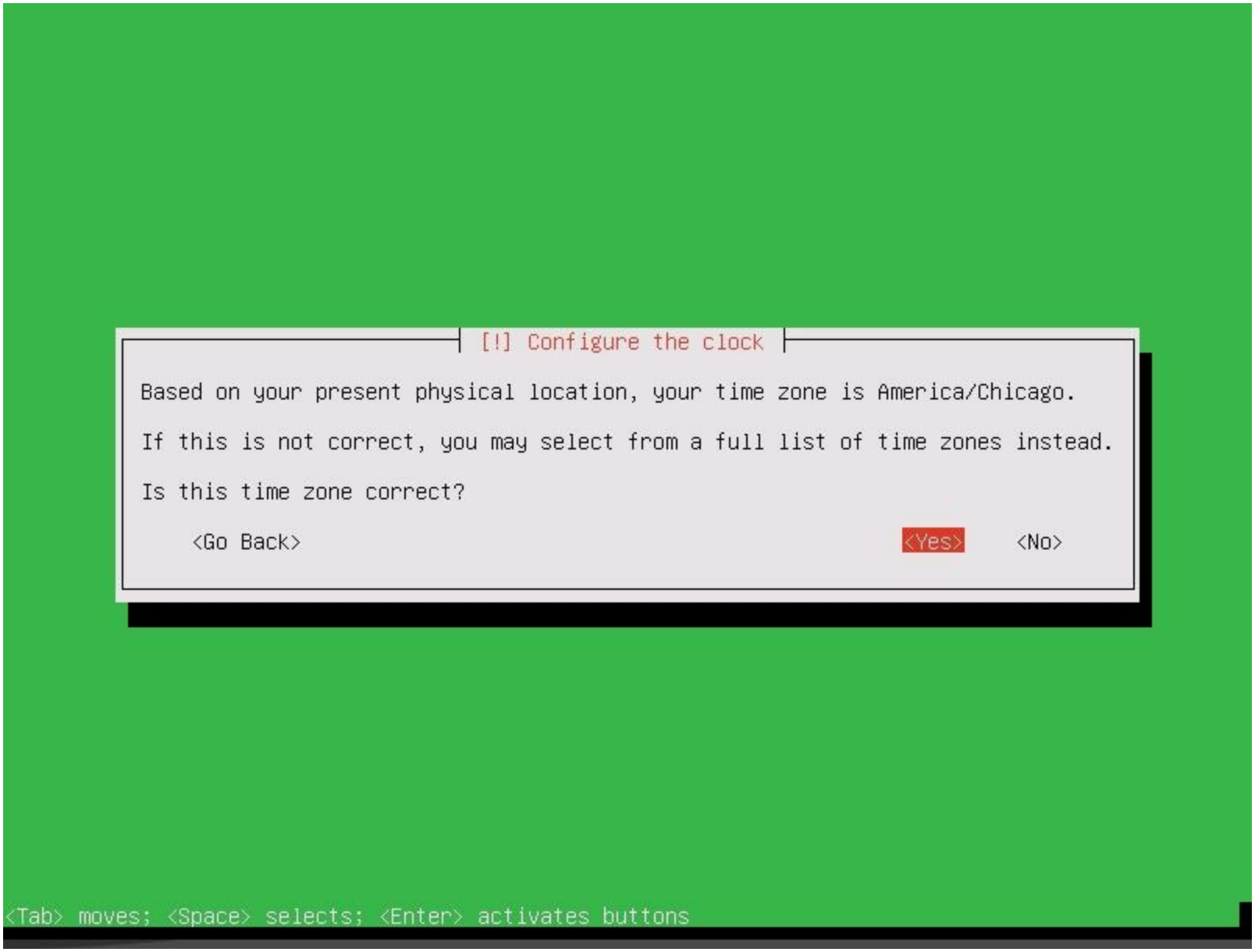
Make sure you choose a strong password to help protect your system(pictured below).

To proceed: Select **Continue** then press **ENTER**



Zentyal should auto-detect your time zone. If it does not then follow the prompt to correct your settings.

To proceed: Select **Yes** then press **<u>ENTER</u>**



When the installation is ready to complete you will be prompted to remove the CD. NOTE: Since this is a VM installation you will do this through the Proxmox interface.

To proceed: Select **Continue** then press **<u>ENTER</u>**

[!!] Finish the installation

Installation complete

Installation is complete, so it is time to boot into your new system. Make sure to remove the installation media (CD-ROM, floppies), so that you boot into the new system rather than restarting the installation.

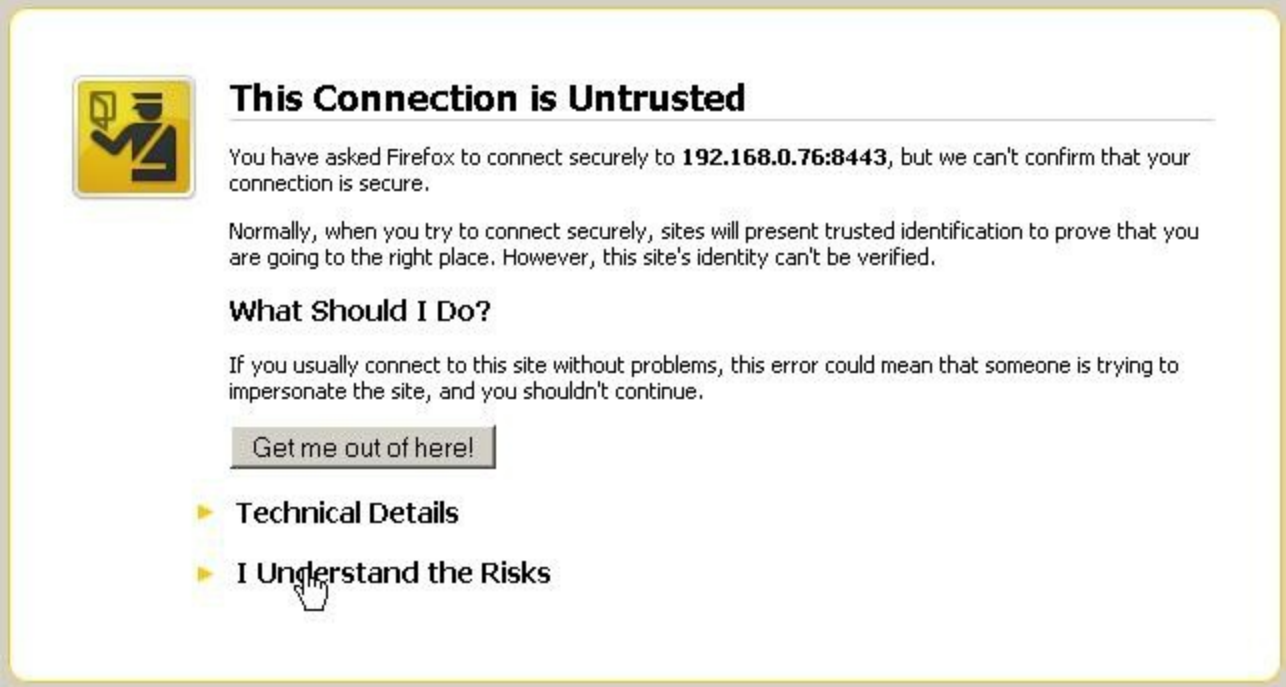
<Go Back> <Continue>

<Tab> moves; <Space> selects; <Enter> activates buttons

4.3-Initial Login

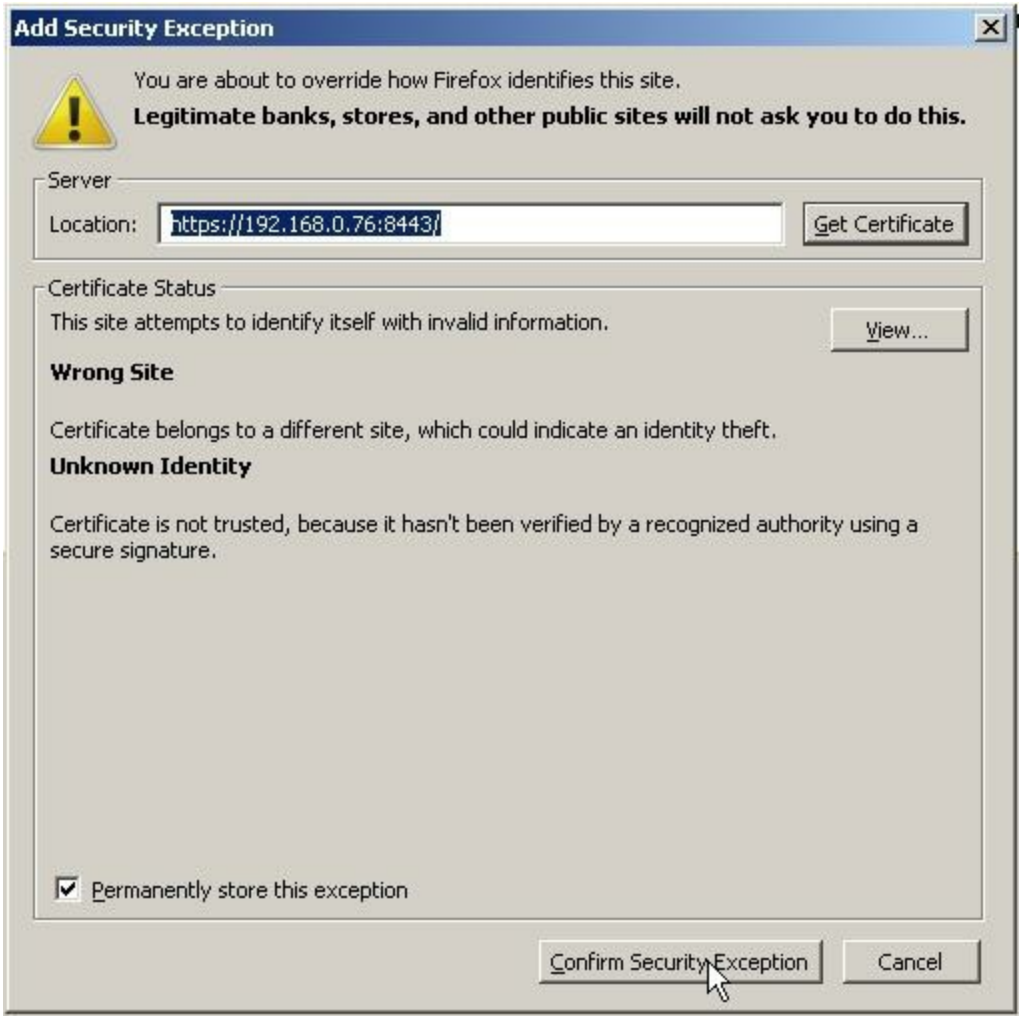
Once Zentyal completes the installation stage it needs to be configured. Enter the IP address for Zentyal in your web browser. This is a secure site so your entry should look something like this: **https://192.168.0.76:8443** For the purpose of this tutorial I have used Mozilla Firefox.

To continue(pictured below): click **I Understand the Risks**



Next: Click ***Add Exception*** as pictured below

Then: Click ***Confirm Security Exception*** as pictured below



You may now login to Zentyal using the credentials established during the installation(pictured below).

4.4-Initial Setup

When you are ready to start the initial setup of Zentyal press the green **Continue** button(shown below).

For our installation we are only using Zentyal as a Domain Controller. When **Domain Controller and File Sharing** is selected a green check will appear(shown below).

To proceed: click **INSTALL**

Package Selection | Installation | Initial Configuration | Save Changes

Choose Zentyal packages to install

Server roles

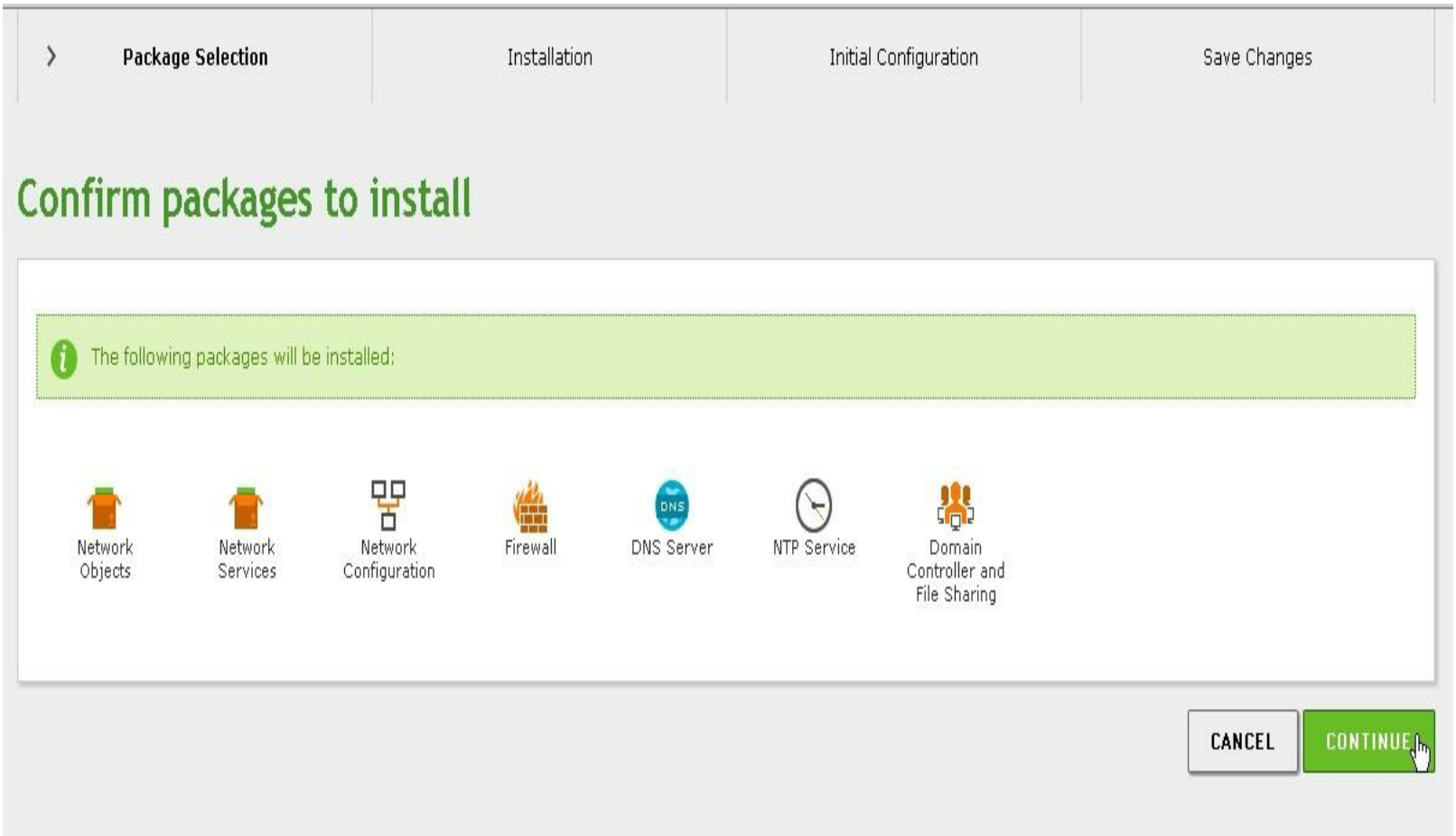
- Domain Controller and File Sharing
- Mail and Groupware
- DNS Server
- DHCP Server
- Firewall

Additional services

- Antivirus
- Certification Authority
- HTTP Proxy
- High Availability
- Jabber
- L2TP
- Mail Filter
- Printers
- Traffic Shaping
- VPN

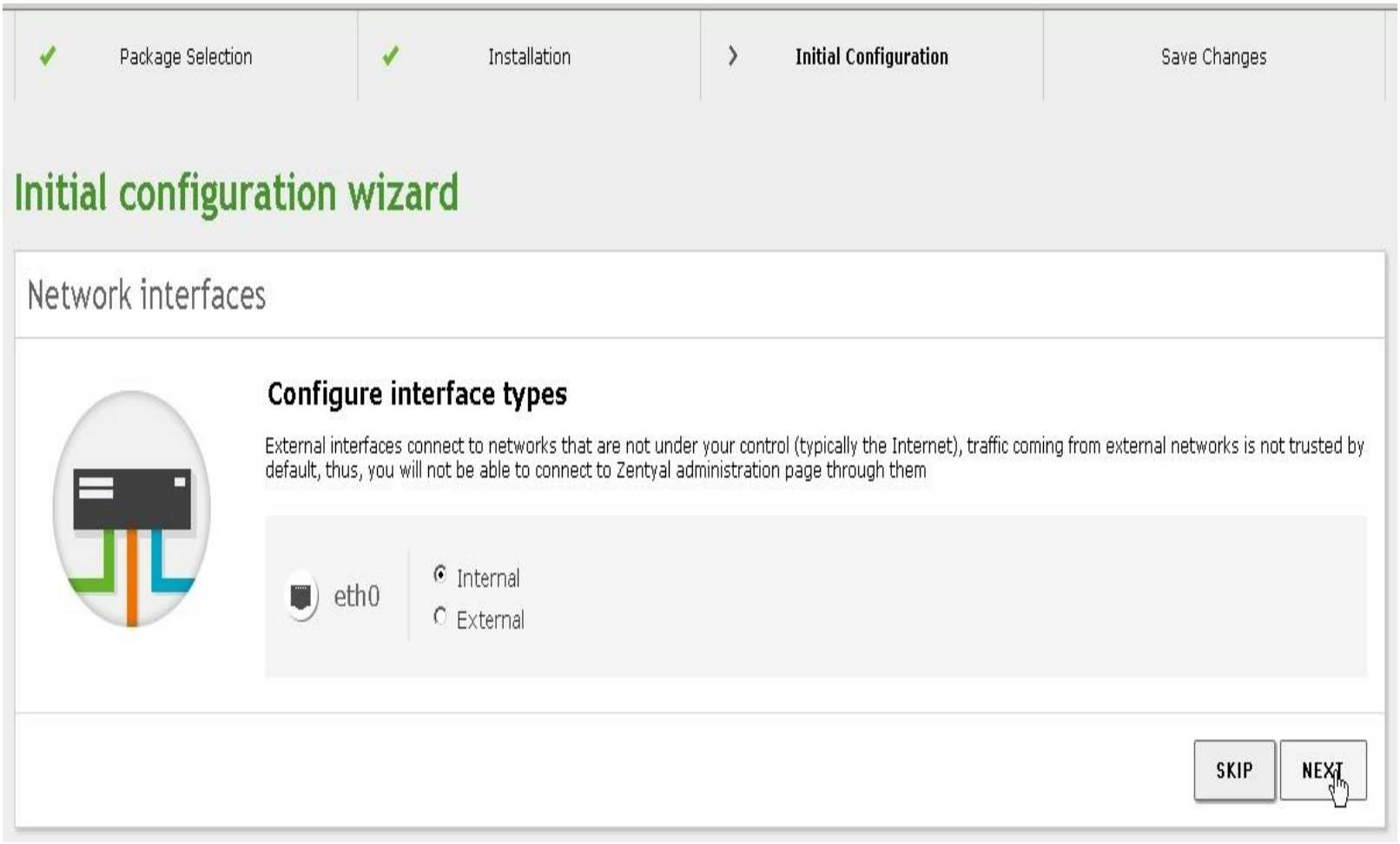
Skip install | INSTALL

Confirm the package selection by clicking **CONTINUE** as shown below.



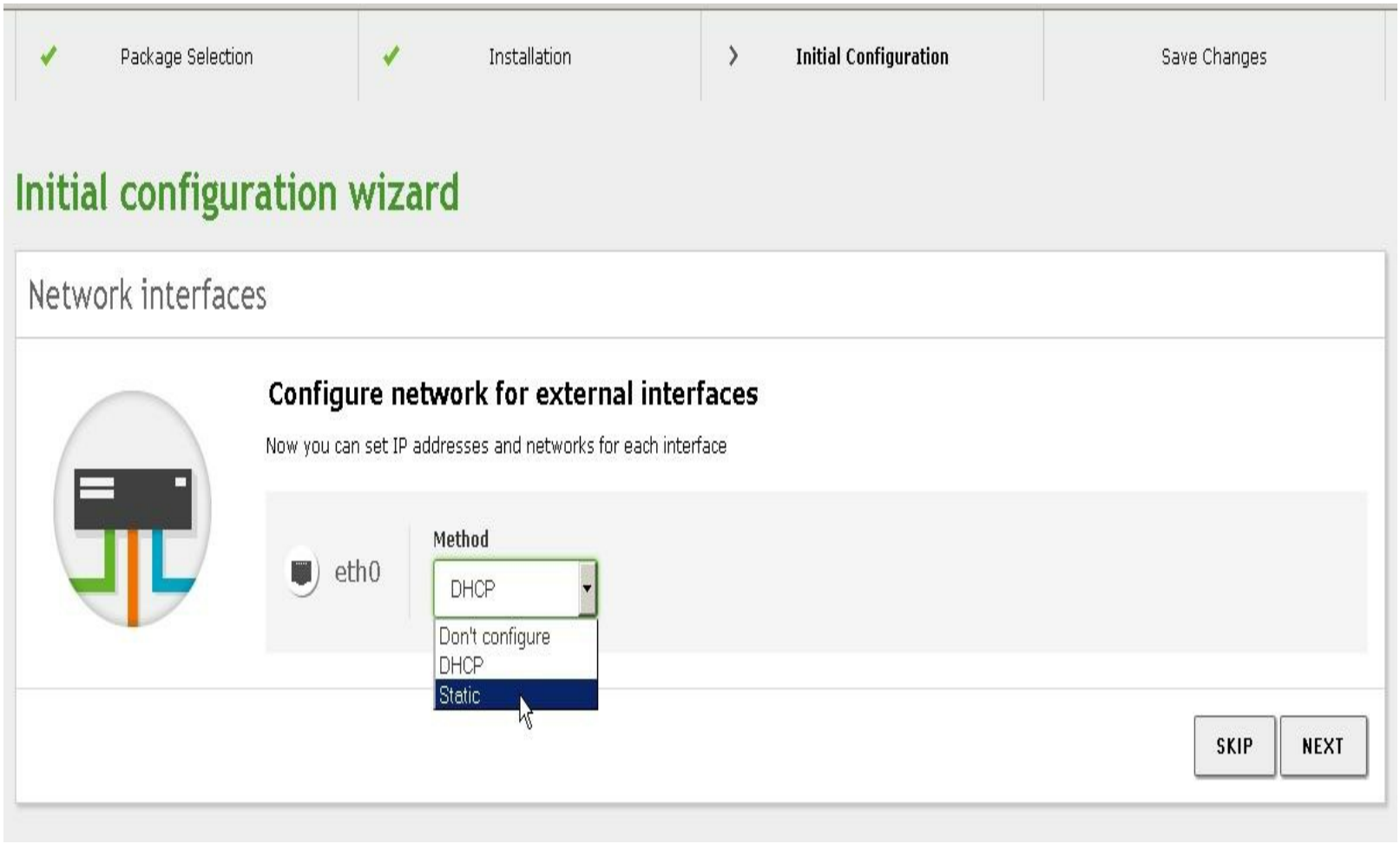
Next, the wizard will prompt to configure network interfaces(shown below).

Select **Internal** for ***eth0*** then click **NEXT**



Since Zentyal is a critical server you will always want a static IP address.

Select **Static** from the dropdown then click **NEXT** to continue(shown below).



Next, enter the appropriate address information(shown below). This should already be populated if you made a DHCP reservation in pfSense.

To proceed: click **NEXT**

Package Selection | Installation | Initial Configuration | Save Changes

Initial configuration wizard

Network interfaces

Configure network for external interfaces

Now you can set IP addresses and networks for each interface

eth0

Method: Static

IP address: 192.168.0.76

Netmask: 255.255.255.0

Gateway: 192.168.0.254

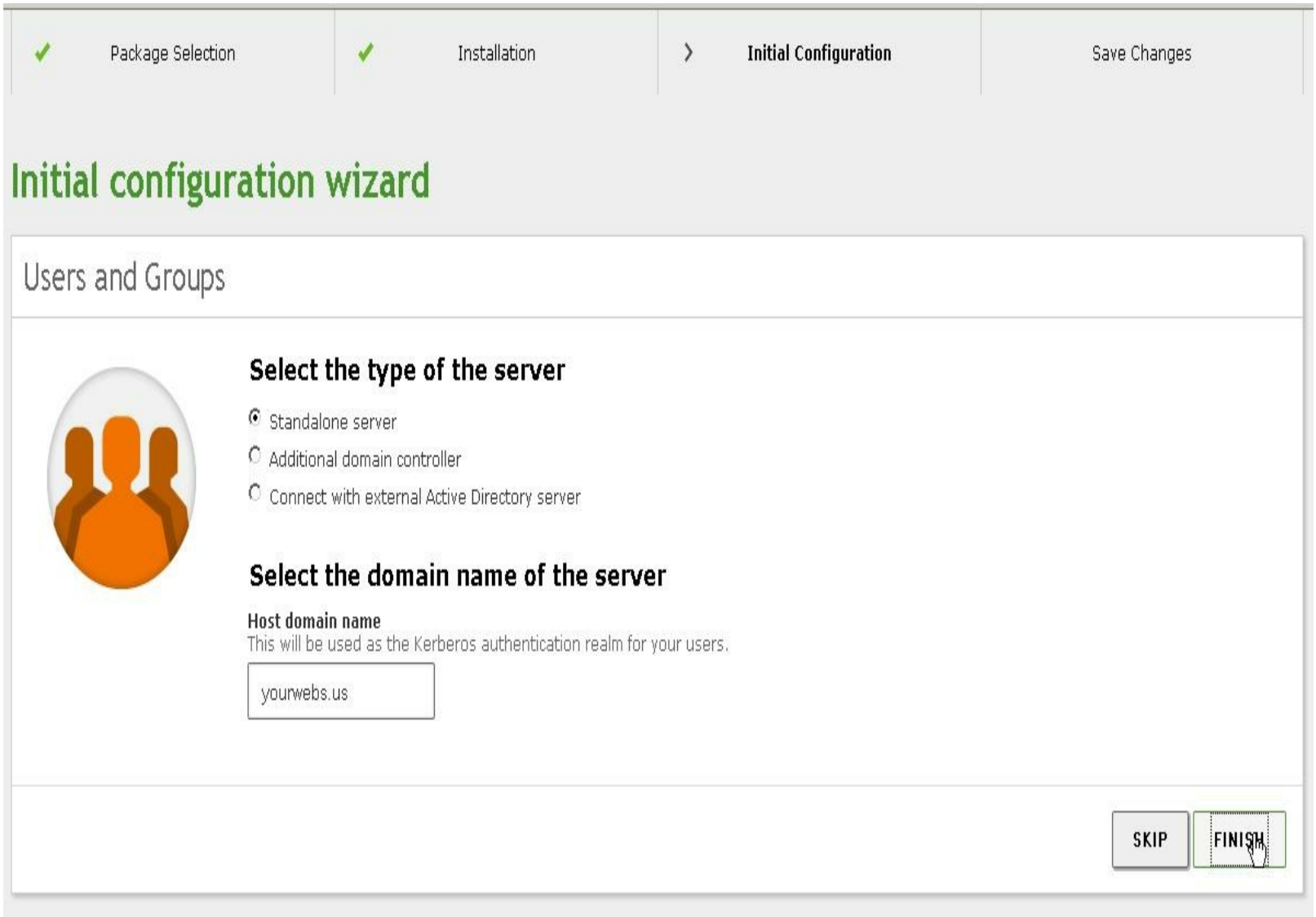
Domain Name Server 1: 192.168.0.254

Domain Name Server 2:

SKIP NEXT

You will now need to enter the **server type** and **domain name** information. For the purpose of this tutorial I have selected a **Standalone** server that authenticates **YOURWEBS.US** users(shown below). **NOTE**: This can easily be changed to Additional domain controller even after the installation is complete. I have included instructions in 4.8-Additional Domain Controller for those who need both PDC and BDC.

To proceed: click **FINISH**



The Zentyal installation is now complete.

To proceed: click **GO TO THE DASHBOARD** (pictured below)

✔ Package Selection ✔ Installation ✔ Initial Configuration ✔ Save Changes

Installation finished

Congratulations!

Your Zentyal installation has successfully finished!

Now you can go to the dashboard and start using your brand new Zentyal server.

GO TO THE DASHBOARD

4.5-Navigating Zentyal

The first screen that appears after final setup or login is the Zentyal Dashboard(pictured below). All further configuration will take place using this interface.

https://192.168.0.76:8443/Dashboard/Index

zentyal Community Edition 4.0

Search...

- Dashboard
- Module Status
- System
- Network
- Logs
- Software Management
- Users and Computers
- Domain
- File Sharing
- DNS
- Firewall

Created by Zentyal S.L.

Dashboard

Zentyal 4.1 is available! UPGRADE NOW

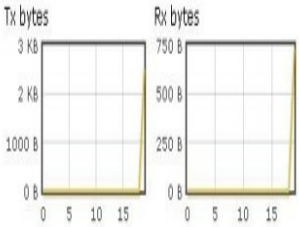
General Information

Time	Mon Dec 21 11:43:51 CST 2015
Hostname	zentyaldc2
Core version	4.0.11
Software	73 system updates (48 security)
System load	0.30, 0.43, 0.31
Uptime	10:53
Users	0

Network Interfaces

eth0

Status	up, internal, link ok
MAC address	26:15:87:a6:07:61
IP address	192.168.0.76



Resources

- Documentation
- Commercial Editions
- Forum
- Certified Training
- Report a bug
- Official Manual

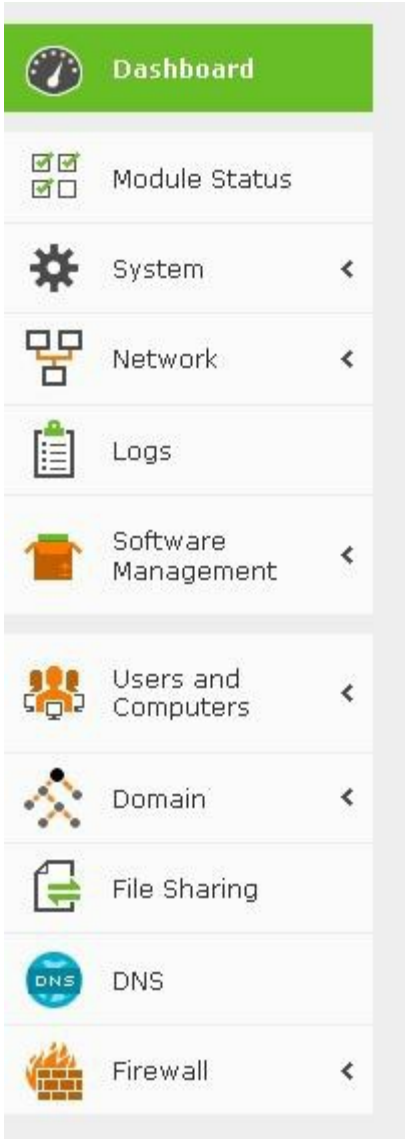
Server Information

Server name	None
Server edition	
Configuration backup	Register to store your backups in the cloud

Module Status

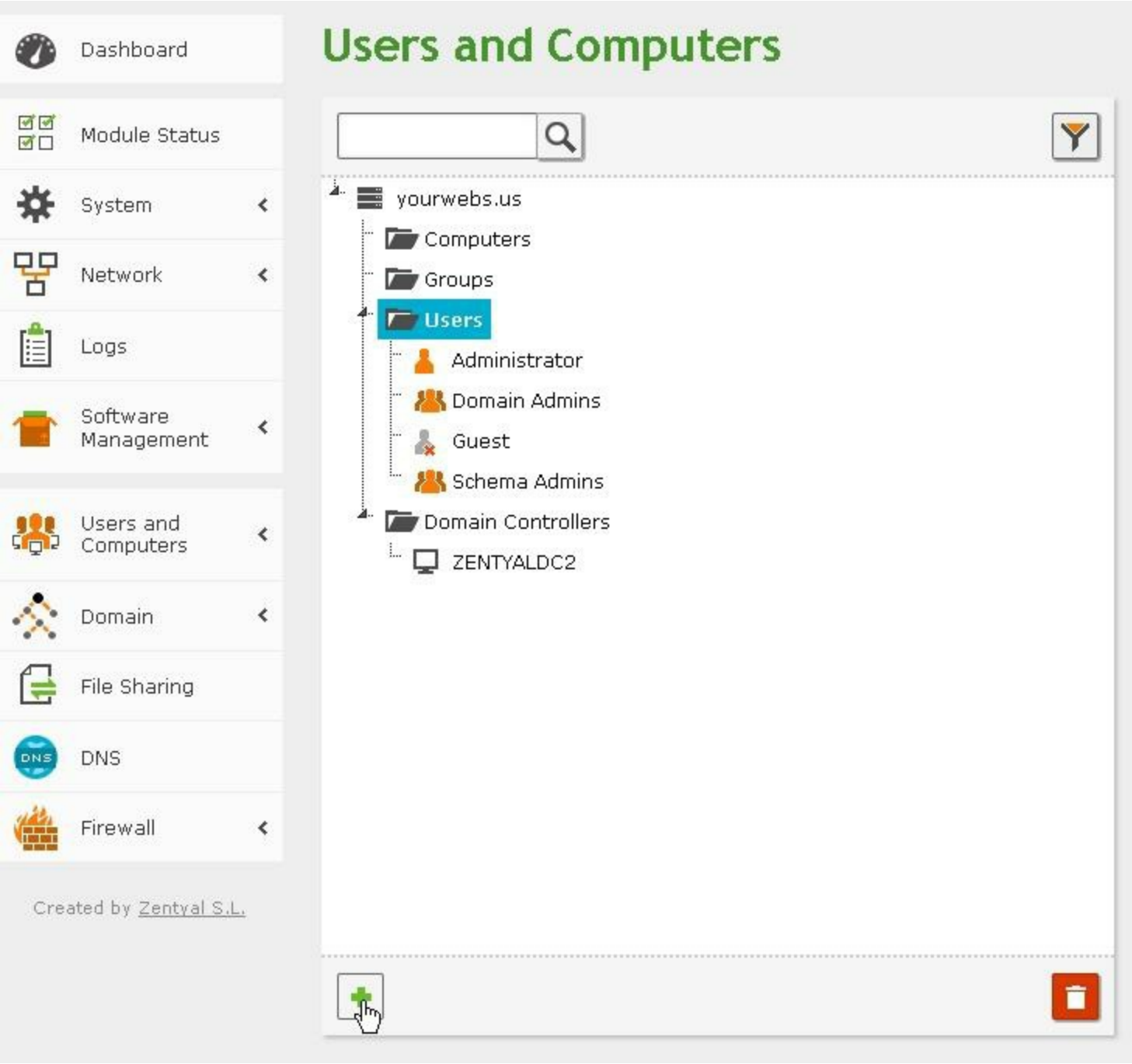
Network	Running	
Firewall	Running	
DNS	Running	Restart
Logs	Running	Restart
NTP	Running	Restart
Domain Controller and File Sharing	Running	

On the left side of the screen you will find the navigation tree(pictured below). When you click on any category in the list it will auto-expand to show additional sub-categories if there are any.



4.6-Adding Users

Adding a user in Zentyal is relatively straight forward. On the left side of the screen click the **Users and Computers** list item. You should now see the **Users and Computers** module screen(shown below). Notice that in our example the ***top level item*** shows the **YOURWEBS.US** domain and all associated items under that domain. To add a new user select the **Users** folder(shown in ***blue*** below). This action will cause the **+ button** at the bottom of the page to turn ***green***(pictured below). Clicking the ***green*** **+ button** will open the Add User dialog.



When the **Add User** dialog appears fill the form with the appropriate information then click **ADD**(shown below).

Add new

- User
- Group
- Contact
- Organizational Unit

Add User

User name

lsurber

First name

Lee

Last name

Surber

Description *Optional*

Author Of This Book

Password

•••••••

Retype password

•••••••

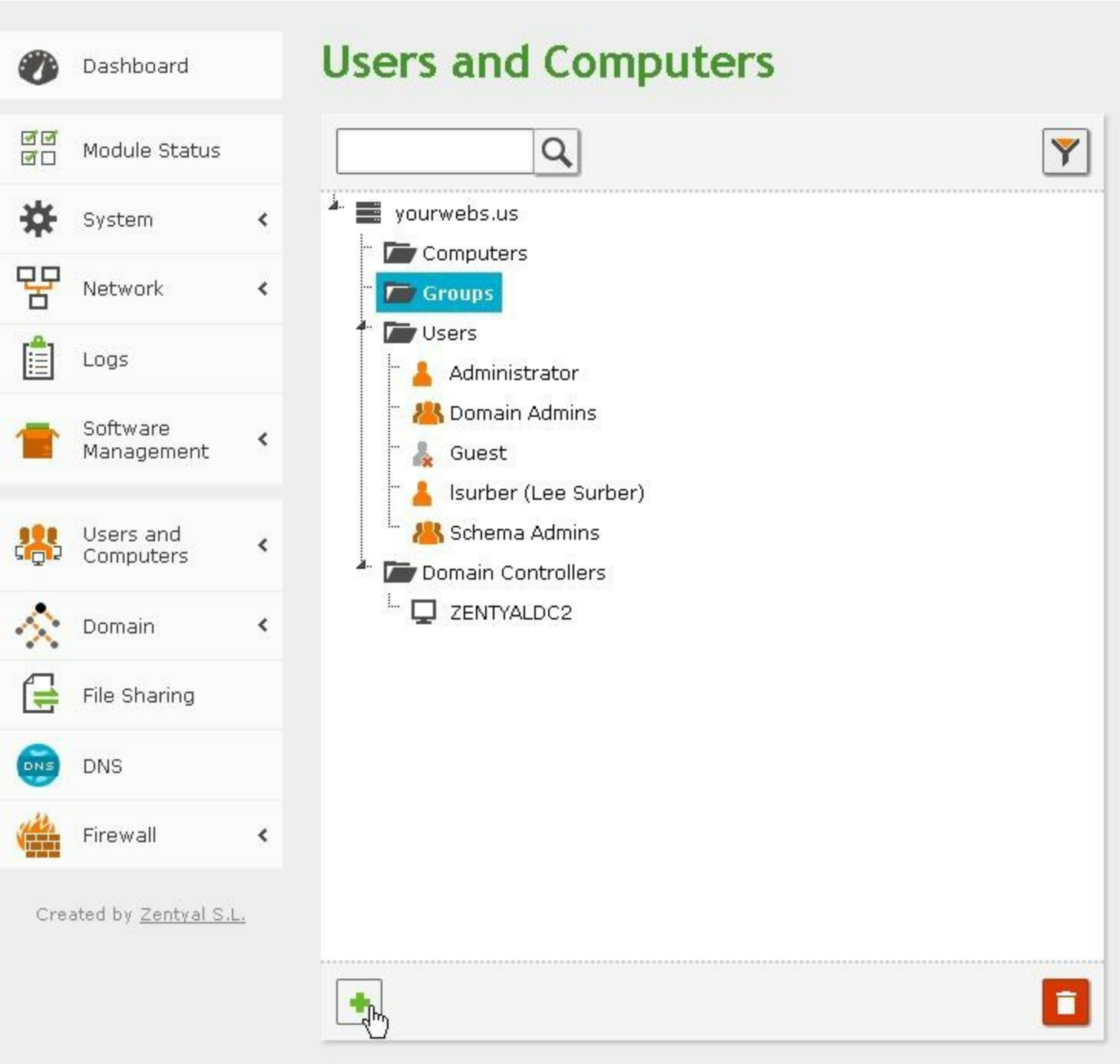
Group

Domain Admins

ADD

4.7-Adding Groups

Adding a group is very much the same as adding a user. On the left side of the screen click the **Users and Computers** list item. You should now see the **Users and Computers** module screen(shown below). Notice that in our example the ***top level item*** shows the **YOURWEBS.US** domain and all associated items under that domain. To add a new group select the **Groups** folder(shown in ***blue*** below). This action will cause the **+ button** at the bottom of the page to turn ***green***(pictured below). Clicking the ***green*** **+ button** will open the Add Group dialog.



When the **Add Group** dialog appears fill the form with the appropriate information then click **ADD**(shown below).

Add new

- User
- Group
- Contact
- Organizational Unit

Add Group

Type

- Security Group
- Distribution Group

Group name

Domain Power Users

Description *Optional value*

E-mail *Optional value*

ADD

4.8-Additional Domain Controller

During installation Zentyal was configured as a ***Standalone*** server named **ZentyalDC2**. This was done purposefully to demonstrate how to ***change the role*** from ***Standalone*** to ***Additional*** domain controller. Let's assume there was already a Zentyal domain controller named **ZentyalDC1** configured as a ***Standalone*** server for the yourwebs.us domain.

To change the **ZentyalDC2** role: Click **Domain>Settings** then select **Additional domain controller** from the dropdown. Enter the information for the ZentyalDC1.yourwebs.us controller as shown below. **IMPORTANT:** The **IP** address **MUST** be that of **ZentyalDC1** and **NOT** that of the **pfSense** router which acts as the DNS server for yourwebs.us. Don't forget to save your changes when finished!

Dashboard

Module Status

System

Network

Logs

Software Management

Users and Computers

Domain

Settings

Group Policy Objects

Group Policy Links

File Sharing

DNS

Firewall

Created by Zentyal S.L.

Domain

Settings

Server Role

Additional domain controller

Realm

yourwebs.us

Domain controller FQDN

zentyaldc1.yourwebs.u

Domain DNS server IP

192.168.0.75

Administrator account

administrator

NetBIOS domain name

yourwebs

NetBIOS computer name

zentyaldc2

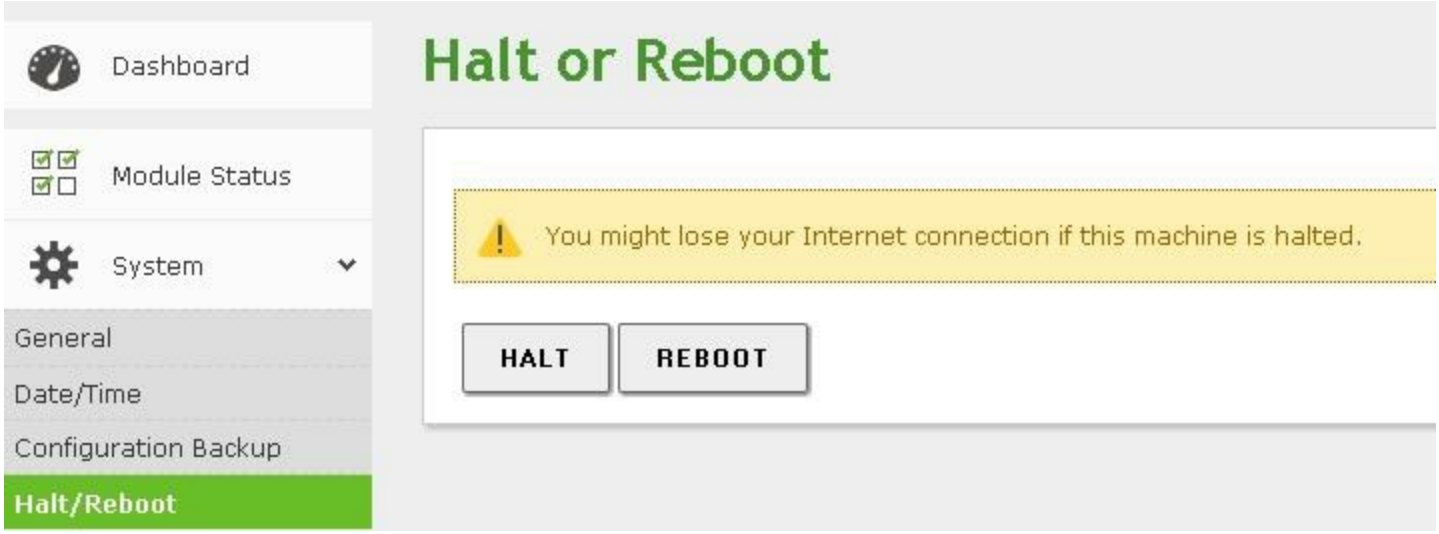
Server description

Zentyal Server2

CHANGE

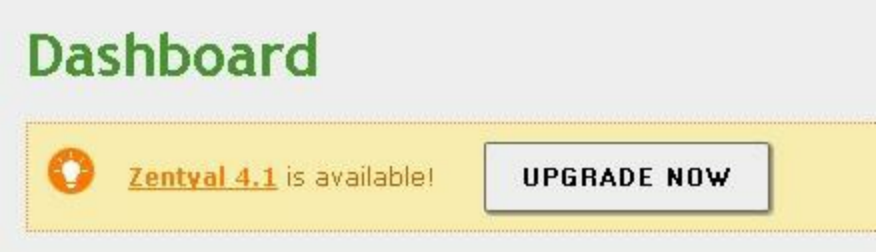
4.9-Shut Down & Reboot

If you should need to shutdown or restart your server that's easy! The control can be found under System in the navigation tree(shown below).



4.10-Upgrading Zentyal

On the main screen you will be alerted when there are upgrades available(shown below). I would strongly recommend against upgrades unless it is absolutely necessary. My preference with Linux based software is to find versions that work and stick with them until a better solution comes along. If it isn't broken don't try to fix it! This really does hold true! In the case of our Zentyal installation it is only being used to hold users in a database. Furthermore, it is virtualized and because of this, will remain compatible for as long as you wish to use it.



4.11-Joining Zentyal Domains

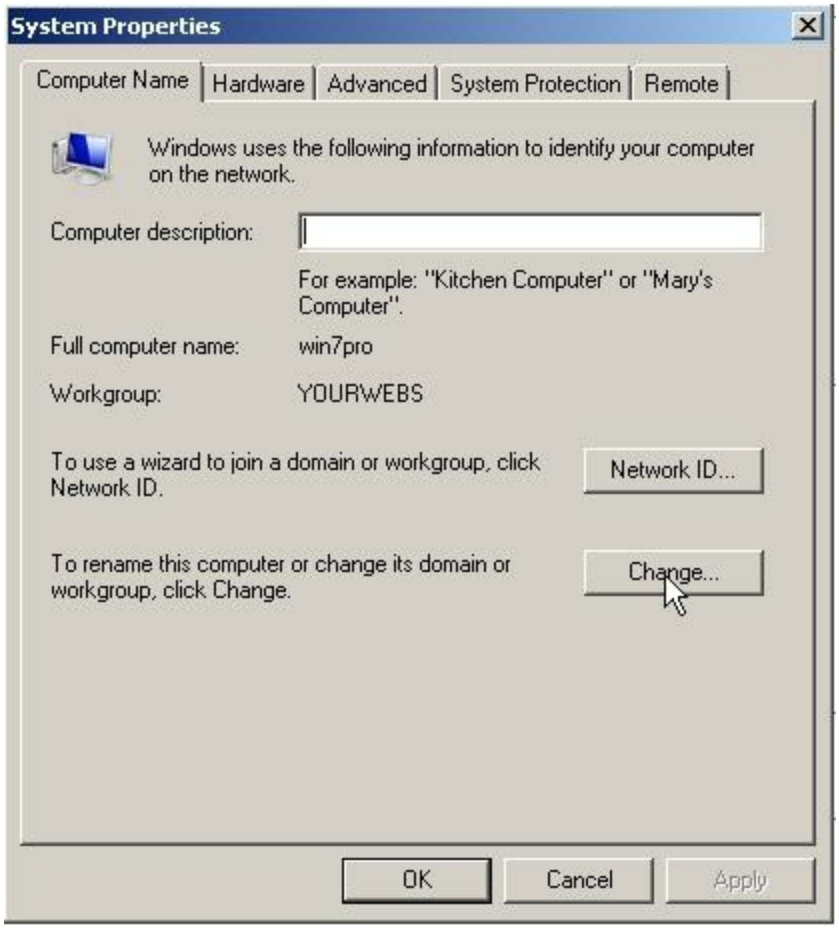
Now that Zentyal is configured for domain control all network clients should be able to ***access*** it. The keyword here is ***access*** NOT ***join***! This is important to understand when administering a domain! The ***common misconception*** is that you must ***join*** a domain to have privilege and that is simply **NOT** the case. In fact, sometimes it may be ***preferred*** to simply remain in a **WORKGROUP** while still having user access to shares that are delegated under a domain. A good example: It is very common for some software to require ***Administrative privilege*** to run. Some very expensive high level CAD software not only require privileges but ***must be run as Administrator***!

Avoiding The IT Dictatorship

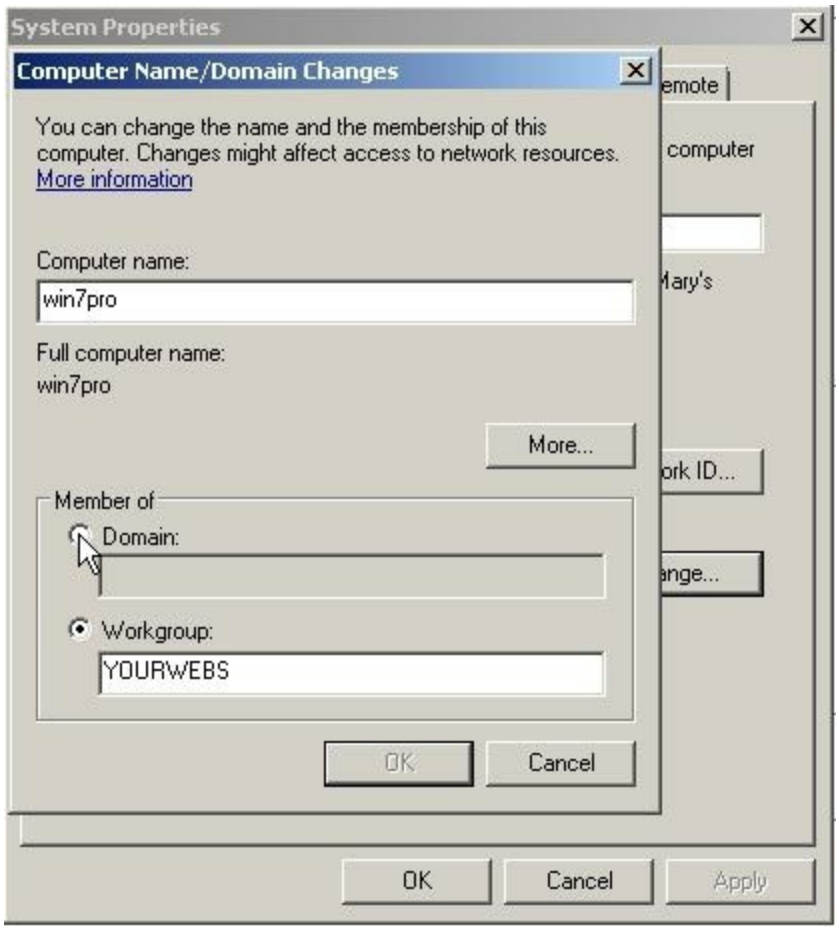
When you elect to join clients to a domain it becomes restrictive and increasingly difficult to manage user preferences. Not all users have the same requirements or preferences. This can make the IT Administrators role very challenging! They must maintain the security and integrity of the system while at the same time not alienating the end users. Using your domain control authority to be overly restrictive can create a hostile workplace where co-workers despise the IT Staff! A properly implemented IDS system running on a layer 2 hardware filtered network will crush just about attack! This allows Administrators to relax user account settings while still maintaining strong network security.

4.11.1-Workgroup Authentication

As mentioned above, it is sometimes preferred to remain in a WORGROUP while still authenticating against a domain. This is by far the simplest system to implement and affords a wide range of flexibility to Admins. Let's take a look at how this works. For the purpose of this book I have a domain named YOURWEBS.US which we have setup Zentyal to be a domain controller for. In the **System Properties>Computer Name** dialog(pictured below) the client workstation is named **win7pro** and the **WORKGROUP** is set to **YOURWEBS**. Essentially, just by **dropping** the domain ***suffix***(**.US**) off the end enables our system to browse network resources that are domain controlled. If you need to change your workgroup name click the **Change** button(shown below) to match the domain name setup in your system.



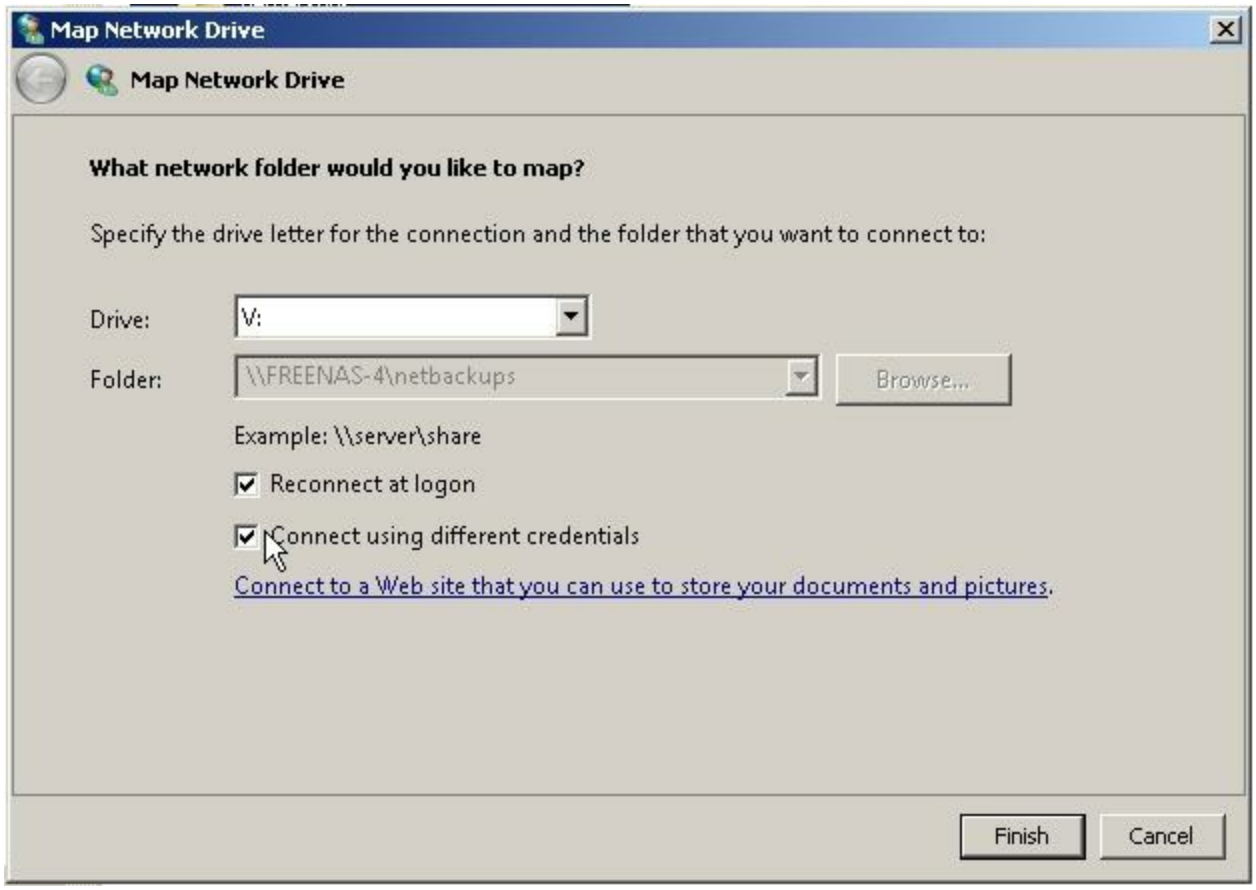
The following dialog appears when you click the Change button above. Simply type your new **Workgroup** name where you see **YOURWEBS**(pictured below) then click **OK**



In Chapter 3.20 we joined our **freeNAS-4** fileserver to the **YOURWEBS.US** so we are already able to take advantage of network share access control. If you need to review freeNAS domain permissions click here: 3.20-Domain Membership Let's map a network share from **freeNAS-4** using **YOURWEBS.US** domain credentials as shown below.

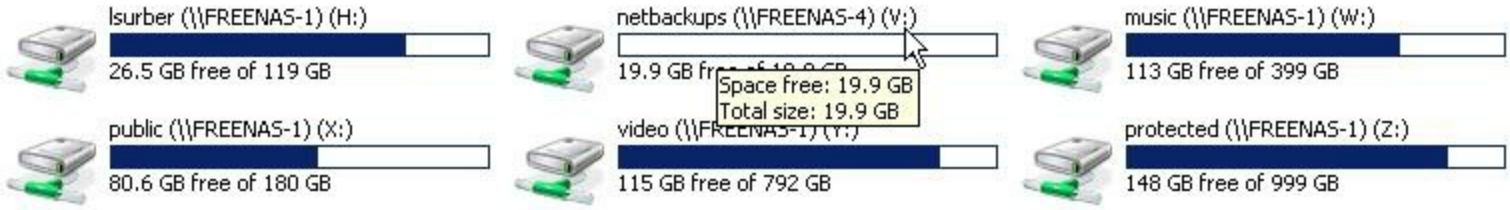
Opening FreeNAS-4 reveals it's share. Simply right click the share then select **Map network drive**(pictured below).

When mapping from a **WORKGROUP** client it is important to check the box ***Connect using different credentials***(shown below).



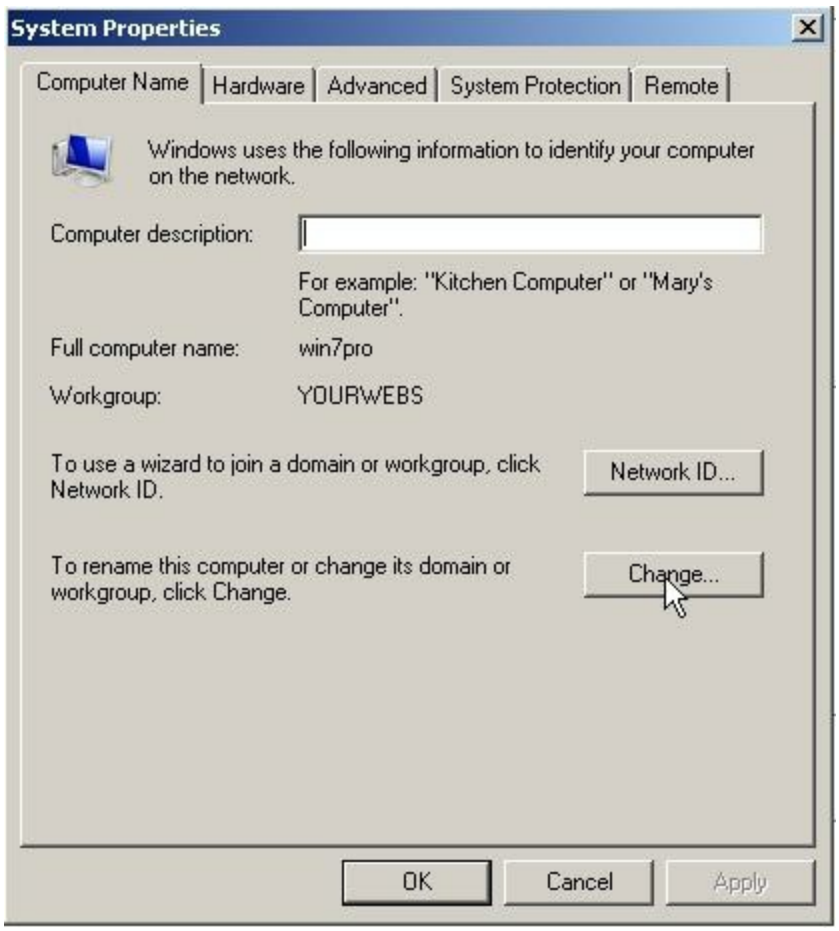
You should then be prompted for the credentials as shown below. Notice that the username **MUST** be formatted to include the domain ***without any suffix*** when connecting from a **WORKGROUP** client. The entry should look something like this: **YOURDOMAIN\username**

After credentials have been accepted you should see your new share mapping(shown below).

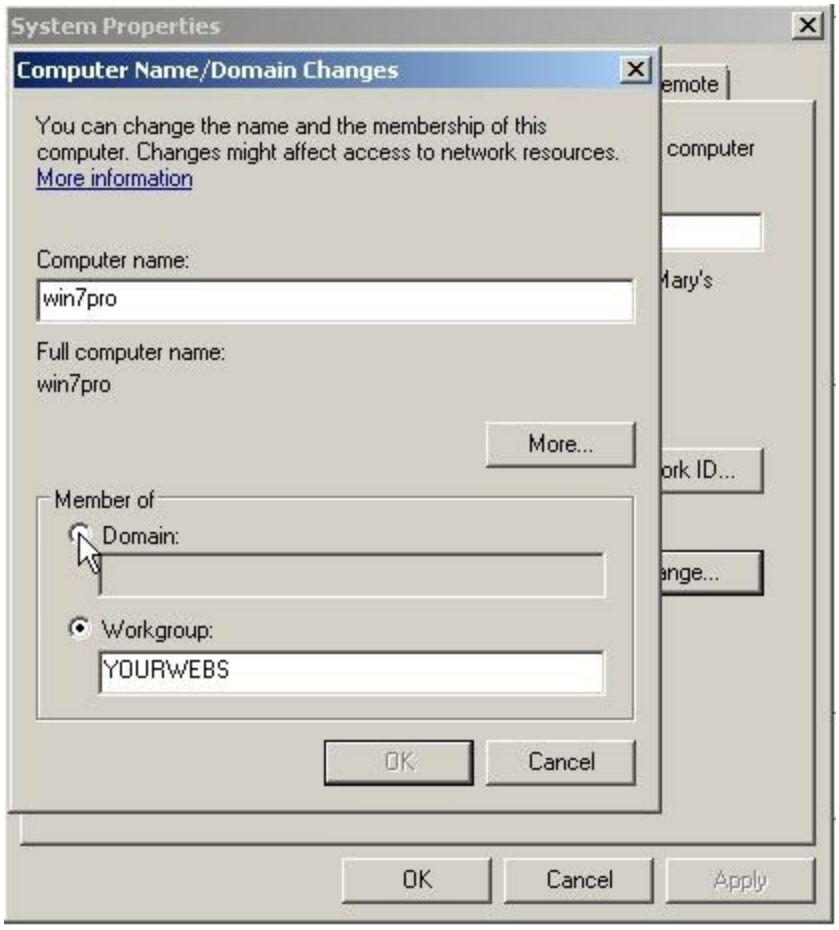


4.11.2-Join The Domain In Windows

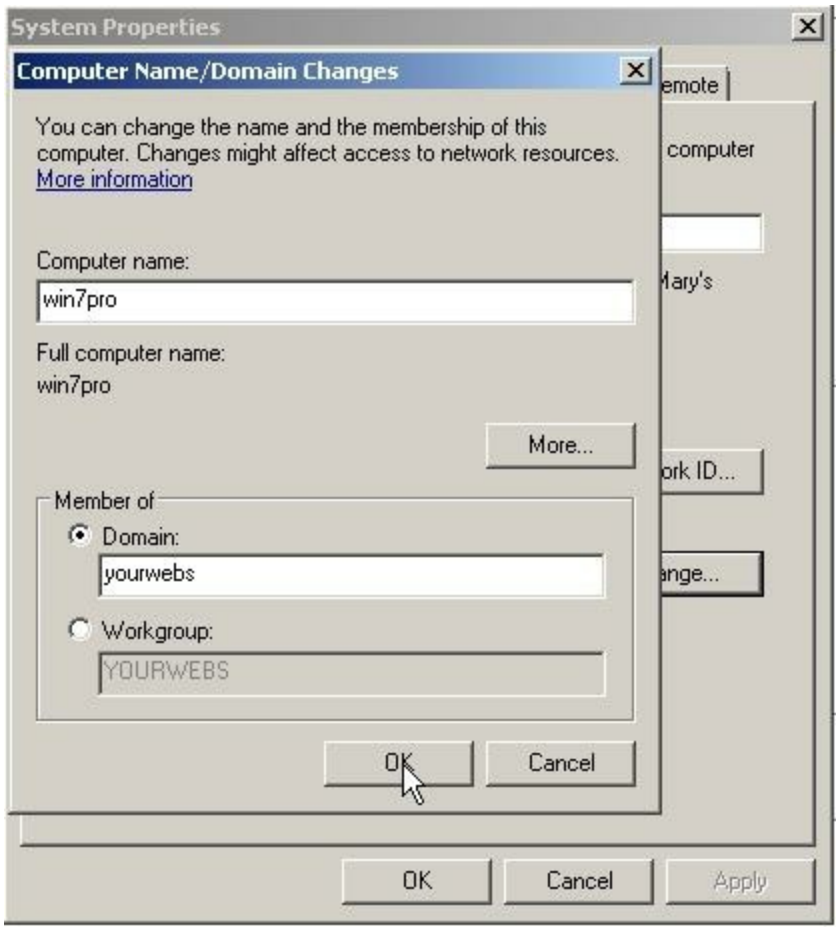
To **join** a network client to the domain is referred to as **binding** and will ***severely*** restrict user preferences. To achieve the bind click the **Change** button(shown below).



Next, select the Domain option(shown below).



Type the domain name **without** any ***suffix***(shown below).



Finally, type the full domain Administrator credentials when prompted. Notice that the username

MUST be formatted to **include** the **full domain** when binding a client. The entry should look something like this: **YOURDOMAIN.XYZ\username**

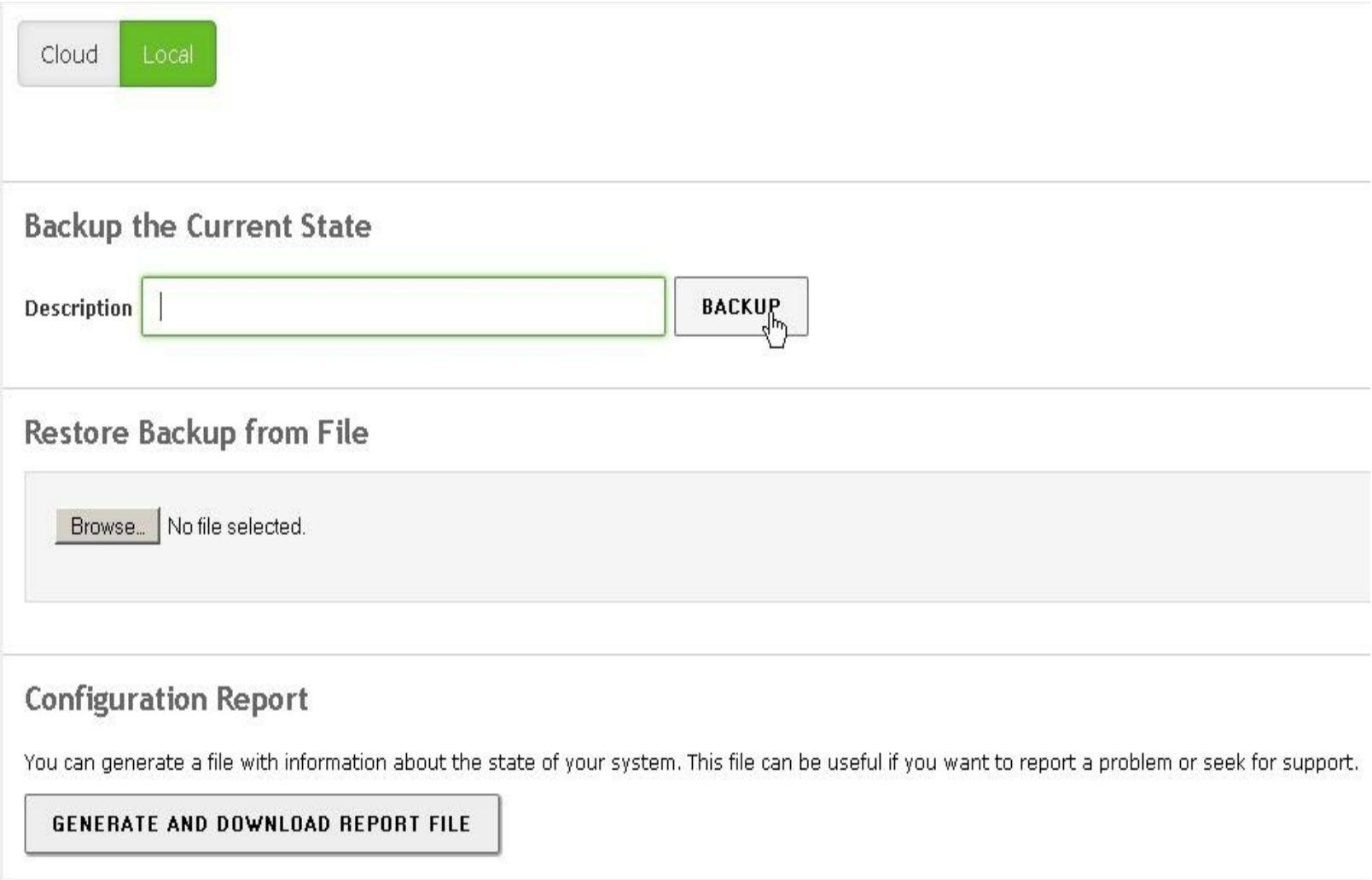
When the client machine is successfully bound you will see the **welcome** dialog after which you will be prompted to **reboot**.

4.12-Configuration Backups

Besides using VM image backups it is also wise to keep a copy of the Zentyal configuration. The configuration backup is especially important when developers rewrite the build in a way that breaks certain packages on update. In these instances your VM image backup will only get you back to the version you were using. I have NOT had this happen with Zentyal, so don't worry too much!

To access the configuration backup page: click **System>Configuration Backup**(pictured below).

Next, select **Local** then click the **BACKUP** button(pictured below).



You should now see your new configuration backup in the **Backups' list**(shown below).

Cloud Local

Backup the Current State

Description BACKUP

Restore Backup from File

Browse... No file selected. RESTORE

Backups' list

Description	Date	Archive size	Actions
Backup	2016-01-13 15:58:57	2.93 MB	

download restore delete

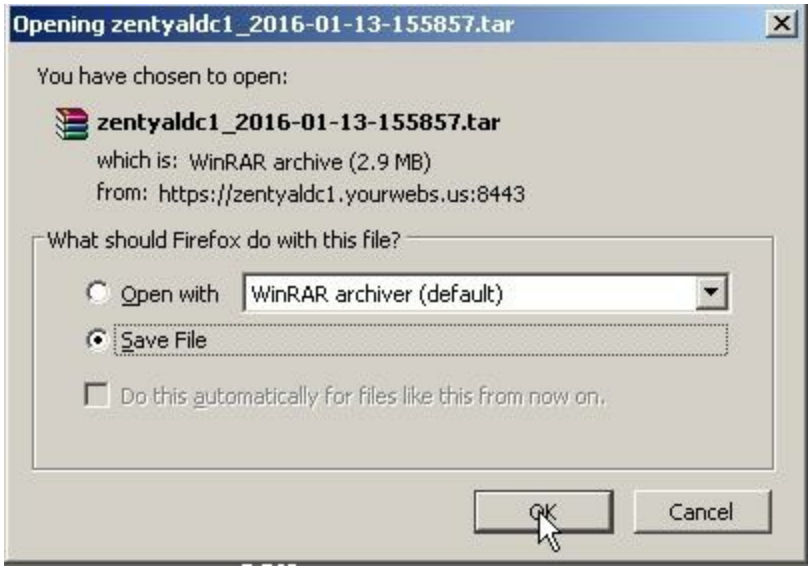
Configuration Report

You can generate a file with information about the state of your system. This file can be useful if you want to report a problem or seek for support.

GENERATE AND DOWNLOAD REPORT FILE

Download your new configuration by clicking the **Download Configuration** button(shown below).

Save your configuration to disk when the download begins. **HINT**: I recommend keeping a copy of this file on thumb drive!



Restoring your Zentyal configuration should be self-explanatory! Simply use the **RESTORE** option instead!

.4-Final Thoughts And Thanks

It doesn't seem too long ago that being an IT Administrator could be hugely stressful. So much so, that I can remember times when I questioned whether or not to remain in the field! I can honestly say that virtualization has changed things for the better! The ease of management and maintenance that it provides has brought back that flame that inspired me so many years ago. I don't think there's a day that passes where I am not awe-inspired with how well this system works! It's like the terminator! Please keep in mind, that none of this would be possible if it were not for the hard work and dedication of the open source development community! So, please! Support the community where you can!

In closing, I would like to thank all those who have purchased and read this book. Many thousands of hours went into production testing and research before I felt confident that this system was ***the system***! I hope that it has been instrumental in building your personal or business based infrastructure. Once you are bitten by the virtualization bug it's seemingly impossible to turn back! For this reason I will continue with future projects focused on an ***even more complete business solution***. Of notable mention, would be my plans to incorporate ***PBX***, ***multi-domain email***, and ***multi-domain webhosting*** servers into this already robust system. So, thanks again and stay tuned for more upcoming ***Virtualization Complete*** releases such as ***BUSINESS PLUS***, ***BUSINESS PRO***, ***BUSINESS ADVANCED***, and perhaps ***ENTERPRISE***!

.5-Additional Resources

www.proxmox.com: Proxmox home page.

www.pfsense.org: pfSense home page.

www.freenas.org: freeNAS home page.

www.zentyal.com: Zentyal home page.

www.distrowatch.com: One of the best open source distribution databases on the web.

Table of Contents

- Book Description
- Copyright
- .1-Introduction
- .2-Before You Begin
- .3-Best Practices
- Book 1: Proxmox VE
  - 1.1-Introduction To Proxmox
  - 1.2-Installing Proxmox
  - 1.3-Initial Login
  - 1.4-Network Adapters
  - 1.5-Adding LVM Storage
  - 1.6-Configure LVM Storage
  - 1.7-Configure NFS Storage
  - 1.8-Configure iSCSI Storage
  - 1.9-Creating VM Configurations
  - 1.10-VM Backup & Restore
  - 1.11-VM Hardware
  - 1.12-Adding Pass-Through Disks
  - 1.13-Troubleshooting Proxmox
  - 1.14-Upgrading Proxmox
- Book 2: pfSense
  - 2.1-Introduction To pfSense
  - 2.2-Installing pfSense
  - 2.3-Assigning Network Interfaces
  - 2.3-Assigning IP Addresses
  - 2.4-Reset Admin Password
  - 2.5-Web Configuration Wizard
  - 2.6-Changing Themes
  - 2.7-Configure DHCP Server
    - 2.7.1-WINS, DNS, Gateway, and Domain
    - 2.7.2-DHCP Client Reservations
  - 2.8-Firewall Settings
    - 2.8.1-LAN Rules
    - 2.8.2-WAN Rules
  - 2.9-OpenVPN
    - 2.9.1-OpenVPN Client Export Utility
    - 2.9.2-OpenVPN Setup Wizard
    - 2.9.3-OpenVPN Client Connectors
    - 2.9.4-Authenticate Zentyal Domain Users
  - 2.10-Snort IDS
    - 2.10.1-Install Snort Package

        - 2.10.2-Snort Global Settings
        - 2.10.3-Snort Interfaces
        - 2.10.4-Updating Threat Rules
        - 2.10.5-Threat Rule Categories
        - 2.10.6-Add Alerts To Suppression List
        - 2.10.7-Block Offenders At Source
    - 2.11-Configuration Backups
- Book 3: freeNAS
    - 3.1-Traditional Storage Fails
    - 3.2-freeNAS & ZFS
    - 3.3-Installing freeNAS
    - 3.4-Add freeNAS Pass-Through Disks
    - 3.5-Set Storage For No Backup
    - 3.6-Start freeNAS Through The Console
    - 3.7-Initial Login
    - 3.8-freeNAS Navigation
    - 3.9-Network Configuration
    - 3.10-Users And Groups
        - 3.10.1-Adding A New User
        - 3.10.2-Adding A New Group
    - 3.11-Add A ZFS Volume
    - 3.12-Detach And Move Volumes
    - 3.13-ZFS Datasets
    - 3.14-ZFS Permissions
    - 3.15-freeNAS Services
        - 3.15.1-CIFS(Windows Sharing) Service
        - 3.15.2-NFS(Linux Sharing) Service
        - 3.15.3-iSCSI Target Service
        - 3.15.4-Rsync(Backup) Service
        - 3.15.5-SSH(Secure Shell) Service
    - 3.16-Add Network Shares
        - 3.16.1-NFS Shares
        - 3.16.2-Windows Shares
        - 3.16.3-iSCSI Target Shares
    - 3.17-ZFS Snapshot Backups
    - 3.18-Restore A Snapshot In Windows
    - 3.19-Rsync Replication
        - 3.19.1-Add The Rsync Push Task
        - 3.19.2-Add The Rsync Module
        - 3.19.3-Tips On Using Rsync
    - 3.20-Domain Membership
        - 3.20.1-Domain Permissions
    - 3.21-Configuration Backups
- Book 4: Zentyal Domain Controller
    - 4.1-Introduction To Zentyal

- 4.2-Installing Zentyal
- 4.3-Initial Login
- 4.4-Initial Setup
- 4.5-Navigating Zentyal
- 4.6-Adding Users
- 4.7-Adding Groups
- 4.8-Additional Domain Controller
- 4.9-Shut Down & Reboot
- 4.10-Upgrading Zentyal
- 4.11-Joining Zentyal Domains
  - 4.11.1-Workgroup Authentication
  - 4.11.2-Join The Domain In Windows
- 4.12-Configuration Backups

- .4-Final Thoughts And Thanks
- .5-Additional Resources

Table of Contents

Book Description
Copyright
.1-Introduction
.2-Before You Begin
.3-Best Practices
Book 1: Proxmox VE
- 1.1-Introduction To Proxmox
- 1.2-Installing Proxmox
- 1.3-Initial Login
- 1.4-Network Adapters
- 1.5-Adding LVM Storage
- 1.6-Configure LVM Storage
- 1.7-Configure NFS Storage
- 1.8-Configure iSCSI Storage
- 1.9-Creating VM Configurations
- 1.10-VM Backup & Restore
- 1.11-VM Hardware
- 1.12-Adding Pass-Through Disks
- 1.13-Troubleshooting Proxmox
- 1.14-Upgrading Proxmox

Book 2: pfSense
- 2.1-Introduction To pfSense
- 2.2-Installing pfSense
- 2.3-Assigning Network Interfaces
- 2.3-Assigning IP Addresses
- 2.4-Reset Admin Password
- 2.5-Web Configuration Wizard
- 2.6-Changing Themes
- 2.7-Configure DHCP Server
  - 2.7.1-WINS, DNS, Gateway, and Domain
  - 2.7.2-DHCP Client Reservations
- 2.8-Firewall Settings
  - 2.8.1-LAN Rules
  - 2.8.2-WAN Rules
- 2.9-OpenVPN
  - 2.9.1-OpenVPN Client Export Utility
  - 2.9.2-OpenVPN Setup Wizard
  - 2.9.3-OpenVPN Client Connectors
  - 2.9.4-Authenticate Zentyal Domain Users
- 2.10-Snort IDS
  - 2.10.1-Install Snort Package
  - 2.10.2-Snort Global Settings

2.10.3-Snort Interfaces
2.10.4-Updating Threat Rules
2.10.5-Threat Rule Categories
2.10.6-Add Alerts To Suppression List
2.10.7-Block Offenders At Source
2.11-Configuration Backups
Book 3: freeNAS
3.1-Traditional Storage Fails
3.2-freeNAS & ZFS
3.3-Installing freeNAS
3.4-Add freeNAS Pass-Through Disks
3.5-Set Storage For No Backup
3.6-Start freeNAS Through The Console
3.7-Initial Login
3.8-freeNAS Navigation
3.9-Network Configuration
3.10-Users And Groups
3.10.1-Adding A New User
3.10.2-Adding A New Group
3.11-Add A ZFS Volume
3.12-Detach And Move Volumes
3.13-ZFS Datasets
3.14-ZFS Permissions
3.15-freeNAS Services
3.15.1-CIFS(Windows Sharing) Service
3.15.2-NFS(Linux Sharing) Service
3.15.3-iSCSI Target Service
3.15.4-Rsync(Backup) Service
3.15.5-SSH(Secure Shell) Service
3.16-Add Network Shares
3.16.1-NFS Shares
3.16.2-Windows Shares
3.16.3-iSCSI Target Shares
3.17-ZFS Snapshot Backups
3.18-Restore A Snapshot In Windows
3.19-Rsync Replication
3.19.1-Add The Rsync Push Task
3.19.2-Add The Rsync Module
3.19.3-Tips On Using Rsync
3.20-Domain Membership
3.20.1-Domain Permissions
3.21-Configuration Backups
Book 4: Zentyal Domain Controller
4.1-Introduction To Zentyal
4.2-Installing Zentyal

4.3-Initial Login
4.4-Initial Setup
4.5-Navigating Zentyal
4.6-Adding Users
4.7-Adding Groups
4.8-Additional Domain Controller
4.9-Shut Down & Reboot
4.10-Upgrading Zentyal
4.11-Joining Zentyal Domains
4.11.1-Workgroup Authentication
4.11.2-Join The Domain In Windows
4.12-Configuration Backups
.4-Final Thoughts And Thanks
.5-Additional Resources