MAGAZINE BSD

FOR NOVICE AND ADVANCED USERS

NetBSD

DEPLOYING NETBSD ON THE CLOUD USING AWS EC2

NETBSD, SAMBA, NFS, AND VSFTPD

HOW TO MANIPULATE IMAGES LIKE A DESIGN PRO

DRAGONFLYBSD AS BACKUP SERVERS IN HIFX

SETUP A VOIP SERVER FOR SIP CALLS

VOL.8 NO.03
ISSUE 03/2014(56)
1898-9144

FREENAS MINI
STORAGE APPLIANCE

IT *SAVES* YOUR LIFE.

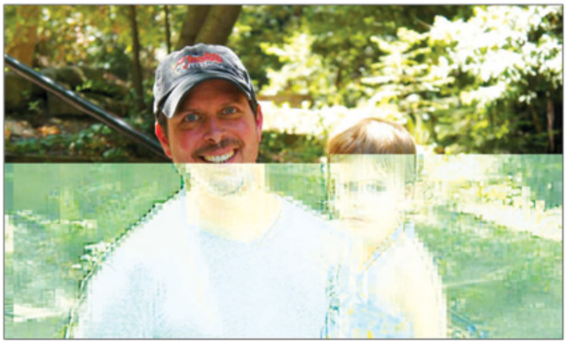
HOW IMPORTANT IS YOUR DATA?

Years of family photos. Your entire music and movie collection. Office documents you've put hours of work into. Backups for every computer you own. We ask again, *how important is your data?*

NOW IMAGINE LOSING IT ALL

Losing one bit - that's all it takes. One single bit, and your file is gone.

The worst part? **You won't know until you absolutely need that file again.**



Example of one-bit corruption

THE SOLUTION

The FreeNAS Mini has emerged as the clear choice to save your digital life. **No other NAS in its class offers ECC (error correcting code) memory and ZFS bitrot protection to ensure data always reaches disk without corruption and *never degrades over time*.**

No other NAS combines the inherent data integrity and security of the ZFS filesystem with fast on-disk encryption. No other NAS provides comparable power and flexibility. The FreeNAS Mini is, hands-down, the best home and small office storage appliance you can buy on the market. **When it comes to saving your important data, there simply is no other solution.**

The Mini boasts these state-of-the-art features:

- 8-core 2.4GHz Intel® Atom™ processor
- Up to 16TB of storage capacity
- 16GB of ECC memory (with the option to upgrade to 32GB)
- 2 x 1 Gigabit network controllers
- Remote management port (IPMI)
- Tool-less design; hot swappable drive trays
- FreeNAS installed and configured

iXsystems®

http://www.iXsystems.com/mini

intel inside™ ATOM™

Intel, the Intel logo, Intel Atom and Intel Atom Inside are trademarks of Intel Corporation in the U.S. and/or other countries.

FREENAS CERTIFIED
STORAGE

With over six million downloads, FreeNAS is undisputedly *the* most popular storage operating system in the world.

Sure, you could build your own FreeNAS system: research every hardware option, order all the parts, wait for everything to ship and arrive, vent at customer service because it *hasn't*, and finally build it yourself while hoping everything fits - only to install the software and discover that the system you spent *days* agonizing over **isn't even compatible**. Or...

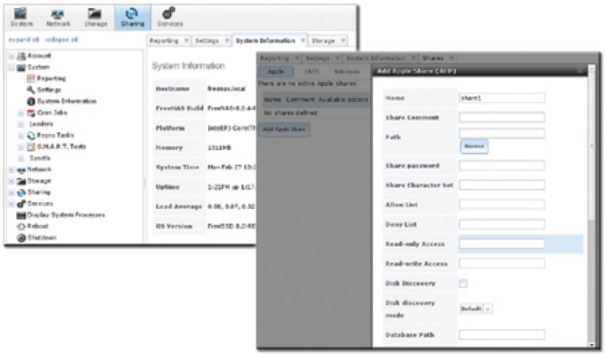
MAKE IT EASY ON YOURSELF

As the sponsors and lead developers of the FreeNAS project, iXsystems has combined over 20 years of hardware experience with our FreeNAS expertise to bring you FreeNAS Certified Storage. **We make it easy to enjoy all the benefits of FreeNAS without the headache of building, setting up, configuring, and supporting it yourself.** As one of the leaders in the storage industry, you know that you're getting the best combination of hardware designed for optimal performance with FreeNAS.

Every FreeNAS server we ship is...

» Custom built and optimized for your use case
» Installed, configured, tested, and guaranteed to work out of the box
» Supported by the Silicon Valley team that designed and built it
» Backed by a 3 years parts and labor limited warranty

As one of the leaders in the storage industry, you know that you're getting the best combination of hardware designed for optimal performance with FreeNAS. **Contact us today for a FREE Risk Elimination Consultation with one of our FreeNAS experts.** Remember, every purchase directly supports the FreeNAS project so we can continue adding features and improvements to the software for years to come. **And really - why would you buy a FreeNAS server from *anyone* else?**



System Information

Hostname freenas.local
FreeNAS Build FreeNAS-8.0.4
Platform Intel(R) Core(T
Memory 1011MB
System Time Mon Feb 27 13:
Uptime 1:21PM up 1:1
Load Average 0.00, 0.07, 0.0
OS Version FreeBSD 8.2-RE

There are no active Apple shares.

Name Comment Available actions
No shares defined

Add Apple Share (AFP)

Name share1
Share Comment
Path
Share password
Share Character Set
Allow List
Deny List
Read-only Access
Read-write Access
Disk Discovery □
Disk discovery mode Default
Database Path

FreeNAS 1U
- Intel® Xeon® Processor E3-1200v2 Family
- Up to 16TB of storage capacity
- 16GB ECC memory (upgradable to 32GB)
- 2 x 10/100/1000 Gigabit Ethernet controllers
- Redundant power supply

FreeNAS 2U
- 2x Intel® Xeon® Processors E5-2600v2 Family
- Up to 48TB of storage capacity
- 32GB ECC memory (upgradable to 128GB)
- 4 x 1GbE Network interface (Onboard) - (Upgradable to 2 x 10 Gigabit Interface)
- Redundant Power Supply

http://www.iXsystems.com/storage/freenas-certified-storage/

Dear Readers,

Hope you are all fine. This issue of BSD magazine is devoted to NetBSD. We worked with highly skilled professionals to give you many valuable articles.

Our opening article is written by Diego Montalvo. He wrote about his own experiences with NetBSD. Working on the development of #pozr, a free developer hosting service, you need to decide to use different flavors of BSD and Linux. Yes Linux... . Diego decided to tell you how to use NetBSD as the web server. In this article Diego will provide you with the steps you will need to deploy your own NetBSD cloud server on AWS EC2. You will learn more about AWS Basics and how to configure an EC2 Instance and how to create a NetBSD Virtual Server.

If you want to read about NetBSD, you need to check the next article: Creating a multi-purpose file server for SOHO business environments with NetBSD, Samba, NFS, and Vsftpd witten by Antonio Francesco Gentile.

In this article Antonio will address two architectures with respect to sharing in the local network: NFS service, historically used in UNIX-like OSes, but now also running on Windows platforms and the Samba service (currently known as CIFS) typical of Windows environments.

In order to manage access to files remotely, the choice fell on the vsftpd daemon configured properly in order to interact with SSL certificates and establish encrypted tunnels in which to flow the traffic data; for example, for connections of type "roadwarrior".

You will find a lot of useful tips here to create the multi-purpose file server.

Please remember to try your skills as a graphic designer and read the next article by Rob Somerville. Rob will continue to look at graphic design basics, and how to use the most popular Open Source graphics software – The Gimp. You will learn in this series how to manipulate images like a design pro.

As always you need to read Rob's next column to see what he prepared for you this time.

Those are just a few of the articles you will find in the magazine. I wish you all good reading and I hope you will learn some new things!

Best regards,
BSD Team

MAGAZINE BSD

Editor in Chief:
Ewa Dudzic
ewa.dudzic@software.com.pl

Contributing:
Michael Shirk, Andrey Vedikhin, Petr Topiarz, Charles Rapenne, Anton Borisov, Jeroen van Nieuwenhuizen, José B. Alós, Luke Marsden, Salih Khan, Arkadiusz Majewski, BEng, Toki Winter, Wesley Mouedine Assaby

Top Betatesters & Proofreaders:
Annie Zhang, Denise Ebery, Eric Geissinger, Luca Ferrari, Imad Soltani, Olaoluwa Omokanwaye, Radjis Mahangoe, Mani Kanth, Ben Milman, Mark VonFange

Special Thanks:
Annie Zhang
Denise Ebery

Art Director:
Ireneusz Pogroszewski

DTP:
Ireneusz Pogroszewski
ireneusz.pogroszewski@software.com.pl

Senior Consultant/Publisher:
Paweł Marciniak
pawel@software.com.pl

CEO:
Ewa Dudzic
ewa.dudzic@software.com.pl

Production Director:
Andrzej Kuca
andrzej.kuca@software.com.pl

Publisher:
Hakin9 Media SK
02-676 Warsaw, Poland
Postepu 17D
Poland
worldwide publishing
editors@bsdmag.org
www.bsdmag.org

Hakin9 Media SK is looking for partners from all over the world. If you are interested in cooperation with us, please contact us via e-mail: editors@bsdmag.org.

NetBSD

GIMP

Column

Deploying NetBSD on the Cloud Using AWS EC2: Part 1

Working on the development of #pozr, a free developer hosting service, I decided to use different flavors of BSD and Linux. Yes Linux... Anyway I decided to use NetBSD as the web server. Having usually used FreeBSD, I am now an equal fan of both BSD distributions.

You will need…

- Amazon AWS account
- Terminal
- OpenSSL

You will learn…

- AWS Basics
- How to configure an EC2 Instance
- Creating a NetBSD Virtual Server

Moving forward in this article I will provide you with the steps you will need to deploy your own NetBSD cloud server on AWS EC2.

Registration and Initial Setup

Register or Log into your Amazon Web Services (AWS) account.

Once you are logged into the AWS account you will see a list of all the AWS offerings. For the sake of simplicity this article will only cover Elastic Cloud Compute (EC2), which provides the deployment services for virtual servers in the cloud. (Figure 1)

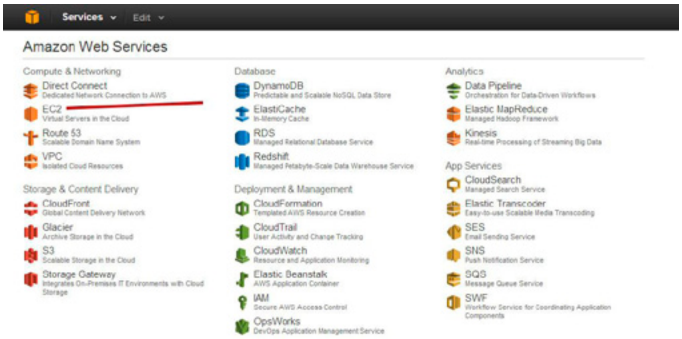
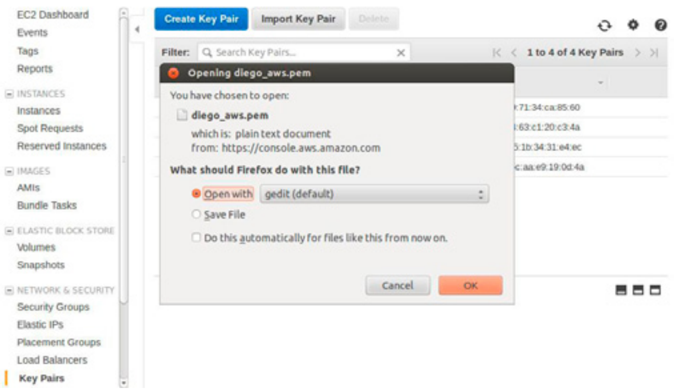

Services
Edit
Amazon Web Services
Compute & Networking
Direct Connect
Dedicated Network Connection to AWS
EC2
Virtual Servers in the Cloud
Route 53
Scalable Domain Name System
VPC
Isolated Cloud Resources
Storage & Content Delivery
CloudFront
Global Content Delivery Network
Glacier
Archive Storage in the Cloud
S3
Scalable Storage in the Cloud
Storage Gateway
Integrates On-Premises IT Environments with Cloud Storage
Database
DynamoDB
Predictable and Scalable NoSQL Data Store
ElastiCache
In-Memory Cache
RDS
Managed Relational Database Service
Redshift
Managed Petabyte-Scale Data Warehouse Service
Deployment & Management
CloudFormation
Templated AWS Resource Creation
CloudTrail
User Activity and Change Tracking
CloudWatch
Resource and Application Monitoring
Elastic Beanstalk
AWS Application Container
IAM
Secure AWS Access Control
OpsWorks
DevOps Application Management Service
Analytics
Data Pipeline
Orchestration for Data-Driven Workflows
Elastic MapReduce
Managed Hadoop Framework
Kinesis
Real-time Processing of Streaming Big Data
App Services
CloudSearch
Managed Search Service
Elastic Transcoder
Easy-to-use Scalable Media Transcoding
SES
Email Sending Service
SNS
Push Notification Service
SQS
Message Queue Service
SWF
Workflow Service for Coordinating Application Components

Figure 1. *Amazon Web Services*

Click on EC2 "Virtual Servers in the Cloud". Before we begin setting up a new virtual server we will have to setup a *Key Pair* which will allow you to access your server using SSH.

Note

If you do not create a Key Pair you will not be able to access your virtual server.



Opening diego_aws.pem

You have chosen to open:

diego_aws.pem

which is: plain text document
from: https://console.aws.amazon.com

What should Firefox do with this file?

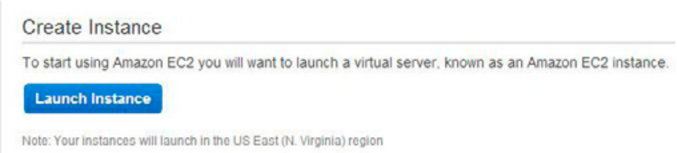
● Open with gedit (default)
○ Save File
□ Do this automatically for files like this from now on.

:71:34:ca:85:60
:63:c1:20:c3:4a
5:1b:34:31:e4:ec
c:aa:e9:19:0d:4a

Figure 2. *Create Key Pair*

In the *NETWORK & SECURITY* section choose the *Key Pairs* option. Next click “Create Key Pair”, name your key and click Yes. You will be prompted to save your newly created *your_key.pem* file; save in a directory. (Figure 2)

We will now begin creating an *Amazon Machine Image* (AMI). Back in the *EC2 Dashboard* click on the “Launch Instance” button. (Figure 3)



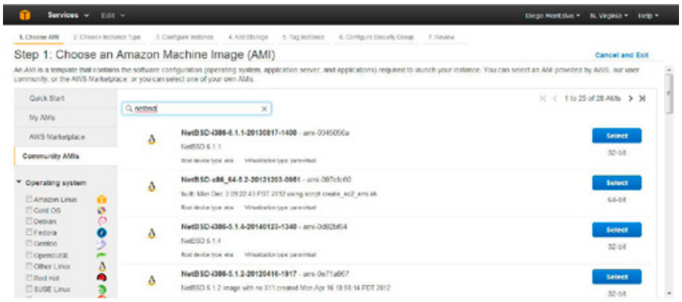
Create Instance

To start using Amazon EC2 you will want to launch a virtual server, known as an Amazon EC2 instance.

Note: Your instances will launch in the US East (N. Virginia) region

Figure 3. *Create Instance*

Inside the *Choose an Amazon Machine Image* screen, we will be accessing Community AMIs and searching for all public NetBSD images. (Figure 4) For this article I chose the following configuration.



Step 1: Choose an Amazon Machine Image (AMI)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. You can select an AMI provided by AWS, our user community, or the AWS Marketplace; or you can select one of your own AMIs.

netbsd

1 to 25 of 28 AMIs

NetBSD-i386-6.1.1-20130817-1400 - ami-0345056a
NetBSD 6.1.1
Root device type: ebs Virtualization type: paravirtual
32-bit

NetBSD-x86_64-5.2-20121203-0981 - ami-097cfc60
built: Mon Dec 3 09:22:43 PST 2012 using script create_ec2_ami.sh
Root device type: ebs Virtualization type: paravirtual
64-bit

NetBSD-i386-5.1.4-20140123-1340 - ami-0d82bf04
NetBSD 5.1.4
Root device type: ebs Virtualization type: paravirtual
32-bit

NetBSD-i386-5.1.2-20120416-1917 - ami-0e71a967
NetBSD 5.1.2 image with no X11 created Mon Apr 16 18:58:14 PDT 2012
32-bit

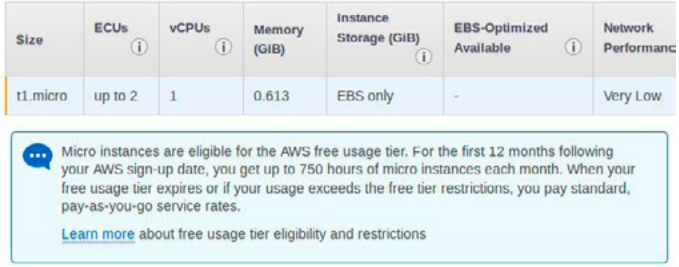
Figure 4. *Choose an AMI*

```
NetBSD-x86_64-6.1.3-20140123-0824   ami-1d90ad74  NetBSD
   6.1.3 64Bit
```

Choose an Instant Type.

Note

Instances range from tiny to very large; the greater the processing power and ram the more you will pay. AWS provides a handy calculator so you can calculate your monthly costs. For new AWS account holders you may enroll in the Free Tier program. (Figure 5)



Size	ECUs ⓘ	vCPUs ⓘ	Memory (GiB)	Instance Storage (GiB) ⓘ	EBS-Optimized Available ⓘ	Network Performanc
t1.micro	up to 2	1	0.613	EBS only	-	Very Low

Micro instances are eligible for the AWS free usage tier. For the first 12 months following your AWS sign-up date, you get up to 750 hours of micro instances each month. When your free usage tier expires or if your usage exceeds the free tier restrictions, you pay standard, pay-as-you-go service rates.

Learn more about free usage tier eligibility and restrictions

Figure 5. *Micro Instances*

Once in *Configure Instance Details* choose an *Availability Zone, us-east-1c* for example. When deploying additional EBS images make sure they are created in the same Availability Zone as your EC2 instance. If not you will not be able to attach the extra storage to your instance.

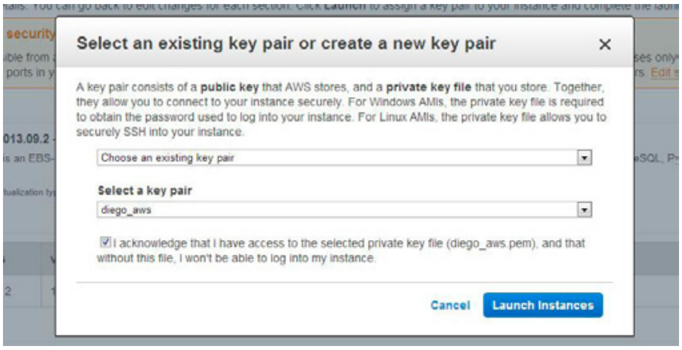
When creating an instance you will be given the option of using Elastic Block Storage (EBS) which in short is an attached storage which is independent of the virtual machine. EBS provides a layer of data protection, for example if your VM becomes corrupted or must be recreated, your EBS can always be reattached to another instance without data loss.

Once in the Configure Security Group screen you will be given the option of using a new or existing security group. I would recommend creating your own; that way you can open and close ports as you see fit.

Note

Security groups work as a firewall between open ports and your instance. For example web traffic on port 80 (0.0.0.0/0) or SSH port 22 (0.0.0.0/0). (0.0.0.0./0) allows traffic from any ip address.

In the last screen before you launch your instance you will be able to review and edit all options. Once you have reviewed your configuration click *Launch*. You will now be prompted to *Select an existing key pair or create a new key pair*. Choose the key pair you created in step four of this tutorial. (Figure 6)



Select an existing key pair or create a new key pair ×

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Choose an existing key pair ▾

Select a key pair

diego_aws ▾

☑ I acknowledge that I have access to the selected private key file (diego_aws.pem), and that without this file, I won't be able to log into my instance.

Figure 6. *Create a New Key Pair*

Check the "I Acknowledge that..." and click *Launch Instances*. The creation process sh – ould take a few minutes. Once the instance is up and running a green dot will appear under the *Instance State* tab of *EC2 Dashboard*.

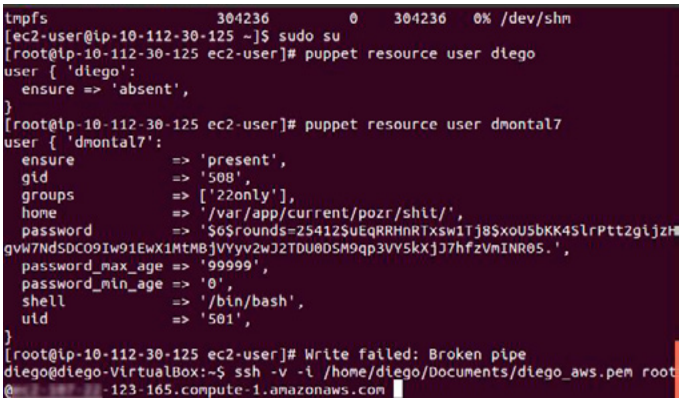
Connecting to Your Instance

Launch the terminal and type the following SSH connection command while changing your pem file location and EC2 public address. (Figure 7)

Resources

Amazon Web Services: *http://aws.amazon.com*
AWS Free Tier Program: *http://aws.amazon.com/free/*
The NetBSD Project: *http://www.netbsd.org/*
NGINX: *http://nginx.org/*

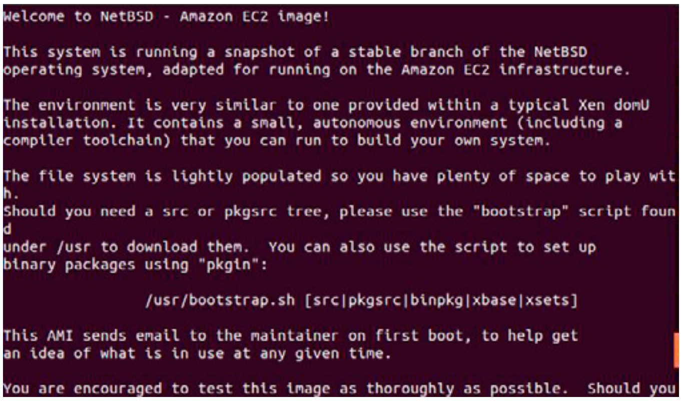
```
# ssh -v -i /your-pem-file_location/diego/diego_aws.pem
   root@ec2-123-12-123-123.compute-1.amazonaws.com
```



```
tmpfs                   304236         0    304236   0% /dev/shm
[ec2-user@ip-10-112-30-125 ~]$ sudo su
[root@ip-10-112-30-125 ec2-user]# puppet resource user diego
user { 'diego':
  ensure => 'absent',
}
[root@ip-10-112-30-125 ec2-user]# puppet resource user dmontal7
user { 'dmontal7':
  ensure           => 'present',
  gid              => '508',
  groups           => ['22only'],
  home             => '/var/app/current/pozr/shit/',
  password         => '$6$rounds=25412$uEqRRHnRTxsw1Tj8$xoU5bKK4SlrPtt2gijzH
gvW7NdSDCO9Iw91EwX1MtMBjVYyv2wJ2TDU0DSM9qp3VY5kXjJ7hfzVmINR05.',
  password_max_age => '99999',
  password_min_age => '0',
  shell            => '/bin/bash',
  uid              => '501',
}
[root@ip-10-112-30-125 ec2-user]# Write failed: Broken pipe
diego@diego-VirtualBox:~$ ssh -v -i /home/diego/Documents/diego_aws.pem root
@[redacted]-123-165.compute-1.amazonaws.com
```

Figure 7. *Terminal*

Upon a successful connection you will be presented with a pleasant *Welcome to NetBSD – Amazon EC2 Instance* screen. (Figure 8)



```
Welcome to NetBSD - Amazon EC2 image!

This system is running a snapshot of a stable branch of the NetBSD
operating system, adapted for running on the Amazon EC2 infrastructure.

The environment is very similar to one provided within a typical Xen domU
installation. It contains a small, autonomous environment (including a
compiler toolchain) that you can run to build your own system.

The file system is lightly populated so you have plenty of space to play wit
h.
Should you need a src or pkgsrc tree, please use the "bootstrap" script foun
d
under /usr to download them.  You can also use the script to set up
binary packages using "pkgin":

                /usr/bootstrap.sh [src|pkgsrc|binpkg|xbase|xsets]

This AMI sends email to the maintainer on first boot, to help get
an idea of what is in use at any given time.

You are encouraged to test this image as thoroughly as possible.  Should you
```

Figure 8. *Welcome to NetBSD Screen*

Having read through this article you should have a basic understanding of AWS EC2 and most importantly a fully functional NetBSD cloud server. In part two of this article, I will cover installation of the NetBSD pkgsrc tree, PHP, Nginx and more. So until next time, keep it moving!

DIEGO MONTALVO

Diego is the chief architect at #pozr. When he is not coding or building web technology, Diego is ranching and skateboarding. He currently resides in both Hebbronville, Texas and San Diego, California. If you have any questions or comments you can contact him at diego@pozr.in.

Creating a Multi-purpose File Server for SOHO Business Environments with NetBSD, Samba, NFS, and Vsftpd

More and more frequently, it is very useful to centralize commonly used files on a dedicated server within the workplace. This particular host is a defined file server, which is where the files containing the templates used for business forms or archives relating to company history are stored. A point in favor of this approach is the fact that using a restricted number of hosts for storage makes it easy to schedule their backups and obtain a copy of important files or simple historical archives.

What you will learn…

- Create a File server with NFS
- Create a File server with CIFS (Samba)
- Create a File server with Vsftpd and SSL Certificates

What you should know…

- Basic network infrastructure concepts
- NetBSD kernel compiling

In the UNIX world, there are different ways to implement file and folder sharing. In particular, in this article we will address two architectures with respect to sharing in the local network:

- NFS service, historically used in UNIX-like OSes, but now also running on Windows platforms
- The Samba service (currently known as CIFS) typical of Windows environments

In order to manage access to files remotely, the choice fell on the vsftpd daemon configured properly in order to interact with SSL certificates and establish encrypted tunnels in which to flow the traffic data; for example, for connections of type “roadwarrior”.

Samba Server Configuration

Samba is a widely used open-source software, which allows users to share resources such as printers and directories between hosts on a network. It basically uses the SMB (server message block) native Microsoft, which itself is based on the NetBios protocol (network basic input output system) developed by IBM. Samba packages are available in the standard repositories, but to have the latest patched version, it’s better to install them using pkgsrc:

```
# cd /usr/pkgsrc/net/samba
```

Then to launch the installer:

```
# make install clean
```

To run Samba, we have to start two services daemons, smbd and nmbd, that are managed by the configuration file `/usr/pkg/etc/samba/smb.conf`.

The configuration parameters are supplied in the form `option = value`; the file is divided into sections that define a share (share), in addition to the general section [global]. Each section is indicated between brackets: [printers]. Comment lines are preceded by an asterisk (#) or semicolon (;). Rows of configuration can span multiple lines smb.conf using a backslash (\) at the end of the line. The options and values are not case sensitive, but if you specify a path in the file system, that is case sensitive. To separate a series of values one can use either a comma (,) or spaces ( ). One can also use variables, preceded by the percent (%) within the values (eg, `path = /home/%u`).

You can include another configuration file in `smb.conf` with the include option (e.g. `include =/usr/pkg/etc/samba/smb.conf.%A`). The configuration options fall under two basic types:

- Global; appear only in the [global] section and define the behavior (very general Samba Server)
- Share; appear in share and define the specific behavior with regard to the specific share. If they appear in the [global] define the default behaviors.

Any option must be included in a section. These are the following special sections:

- [global] Always present, usually at the beginning of the file. Defines the default options that apply to all shares (can be overridden by options otherwise present in the specific sections) and the general parameters of the server configuration.
- [printers] A special section used to share network access to printers
- [homes] A special section that coincides with the home directory of an authenticated user. In fact it is sharing with the generic name of the user who logs on to Samba.
- workgroup: SAMBA information that must enter the linux machine in the specified group ;
- printing: set to allow Samba to use any configuration for printers;
- Load printers: loads the list of printers managed by the printing daemon.
- netbios: the name by which the server is visible on the network.
- security: set to 'USER'; only authorized users can access via password.
- Allow hosts: indicates the networks where the service is made available;
- Username map: mapping files between samba and system users;
- Server string: label that describes the function of the server;
- Create mask: managing default permissions on files created in the shares;
- Smb passwd file: A file that stores your login credentials;

Listing 1. *Samba configuration file commented line by lineThe [global] section*

```
[global]
workgroup = wg_name;
guest account = nobody;
netbios = NBSDSMBSRV
load printers = yes
printing = bsd
printcap name = /etc/printcap
force printername = yes
security = USER
allow hosts = 127.0.0.1 192.168.88.0/24
username map = /usr/pkg/etc/samba/smbusers
server string = DATA SERVER
create mask = 0755
smb passwd file = /usr/pkg/etc/samba/smbpasswd
```

The [homes] section

This section allows users logged on the Windows machine to access their Home Directory Linux.

```
[homes ]
Comment = Home directory
browsable = no
read only = no
printable = no
create mode = 0750
```

- comment: configures the comment of the shared directory on the Windows client;
- browsable: set to no prevents the resource to be viewed by all users;
- read only: enables you to write to the directory;
- printable: if it is not a printer you do not enable this field;
- create mode: all files created by the user will have windows of these preconfigured allowed here.

The [public] share

```
[public]
comment = Public Directory
path = /usr/local/share
browsable = yes
read only = no
public = yes
create mode = 0777
```

The directory `/usr/local/share` will have the following characteristics:

- Will be “visible” and usable by everyone,
- Will be writable
- The files that will be stored will have rwx permissions for everyone.

The [printers] section

```
[printers ]
comment = Printer
path = /var/spool/samba
printable = yes
use client driver = yes
browsable = yes
```

Listing 2. *A simple Samba configuration file for a small LAN*

```
# Soho LAN smb.conf

[global]
   workgroup = MYGROUP
   server string = Samba %v (%h)
   security = user
   load printers = yes


[homes]
   comment = Home Directories
   browseable = no
   writable = yes

[ShareReadOnly]
   comment = DirectorY Read Only
   path=/usr/shared
   browseable = no
   writable = no
   browseable = yes
   valid users = user1
```

To access the print queues to change permissions on the directory:

```
chmod a + rwx /var/spool/samba
```

- It sets the folder as “Printers”
- You specify the path
- Specifies that it is a print spooler
- Forces you to use the drivers installed on the client
- Emerges as visible by all users

```
[HP -1220 ]
comment = USB HP 1220 Printer
path = /var/spool/samba
browseable = yes
```

- HP -1220: Indicates the shared printer queue;
- Comment: description of the print queue;
- Path: path to the files of the print queue;
- Browseable: yes is set to be visible to all users.

To automatically start the services at boot time, you must edit `/etc/inetd.conf` and uncomment the lines:

```
netbios-ssn stream tcp nowait root /usr/pkg/sbin/smbd
netbios-ns dgram udp wait root /usr/pkg/sbin/nmbd
```

then restart inetd with:

```
/etc/rc.d/inetd restart
```

And finally add the following lines to `/etc/rc.conf`:

```
smbd=YES
nmbd=YES
samba=YES
winbindd=YES
```

Here is one simple example of a configuration for a small LAN: Listing 2. To test the Samba setup, one has to add a valid user to the NetBSD system:

```
# useradd user1
```

Add a Windows user to Samba and set the password:

```
# smbpasswd -a -U user1
```

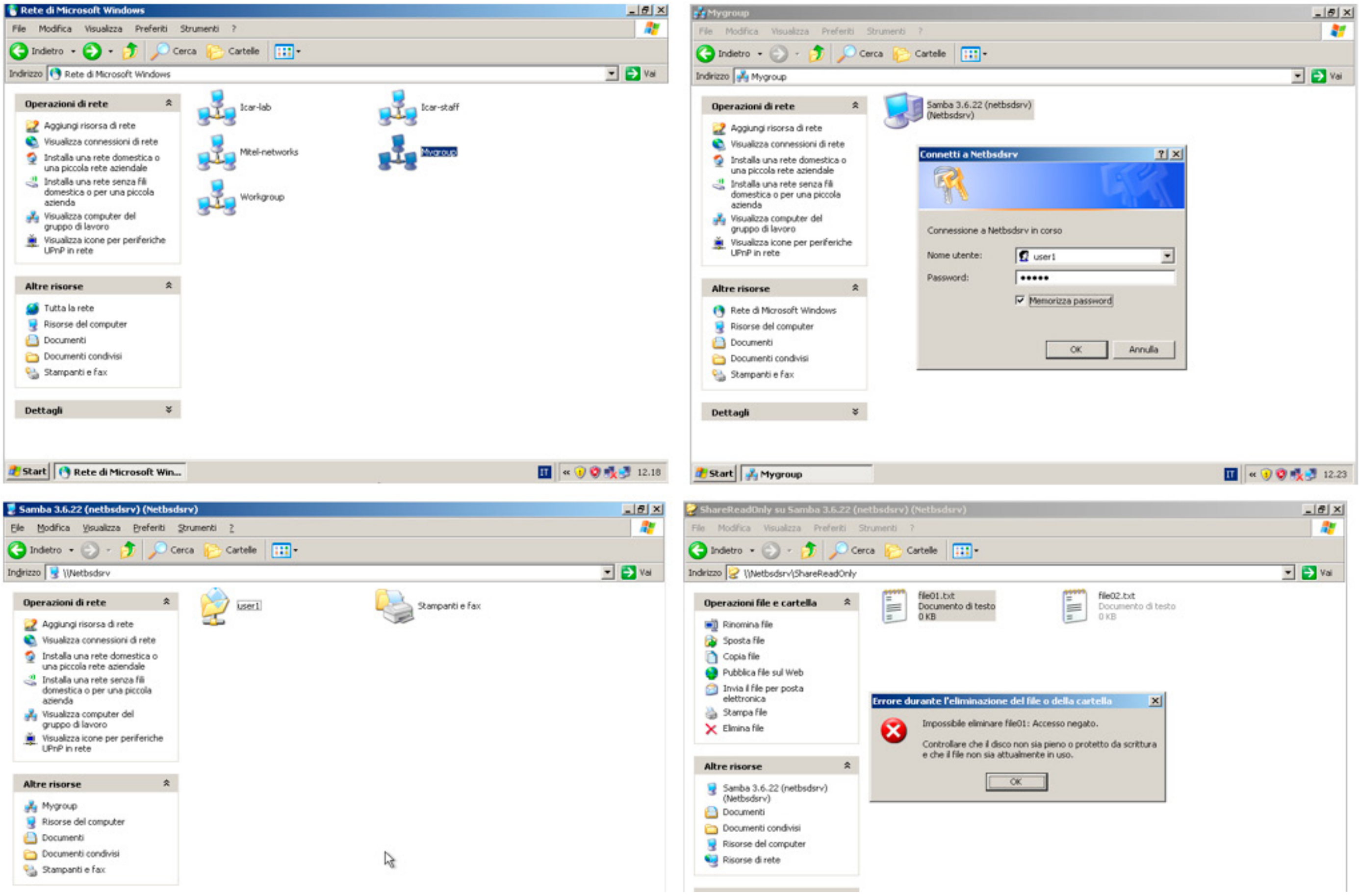
Now test the server with your Windows machine. You can also browse the content from a windows machine with NetBSD smbclient:

```
# smbclient //NbsdSmbSrv/shared_folder
```

NbsdSmbSrv is the IP for the windows machine and shared_folder is the shared directory.

You can also test if your local Samba server is working (see Figure 1-3).

```
# smbclient -U user1 -L localhost
```


Rete di Microsoft Windows
Icar-lab
Icar-staff
Mitel-networks
Mygroup
Workgroup
Mygroup
Samba 3.6.22 (netbsdsrv) (Netbsdsrv)
Samba 3.6.22 (netbsdsrv) (Netbsdsrv)
user1
Stampanti e fax
ShareReadOnly su Samba 3.6.22 (netbsdsrv) (Netbsdsrv)
\\Netbsdsrv\ShareReadOnly
file01.txt
Documento di testo
0 KB
file02.txt
Documento di testo
0 KB

Connetti a Netbsdsrv

Connessione a Netbsdsrv in corso

Nome utente: user1

Password: •••••

☑ Memorizza password

OK Annulla

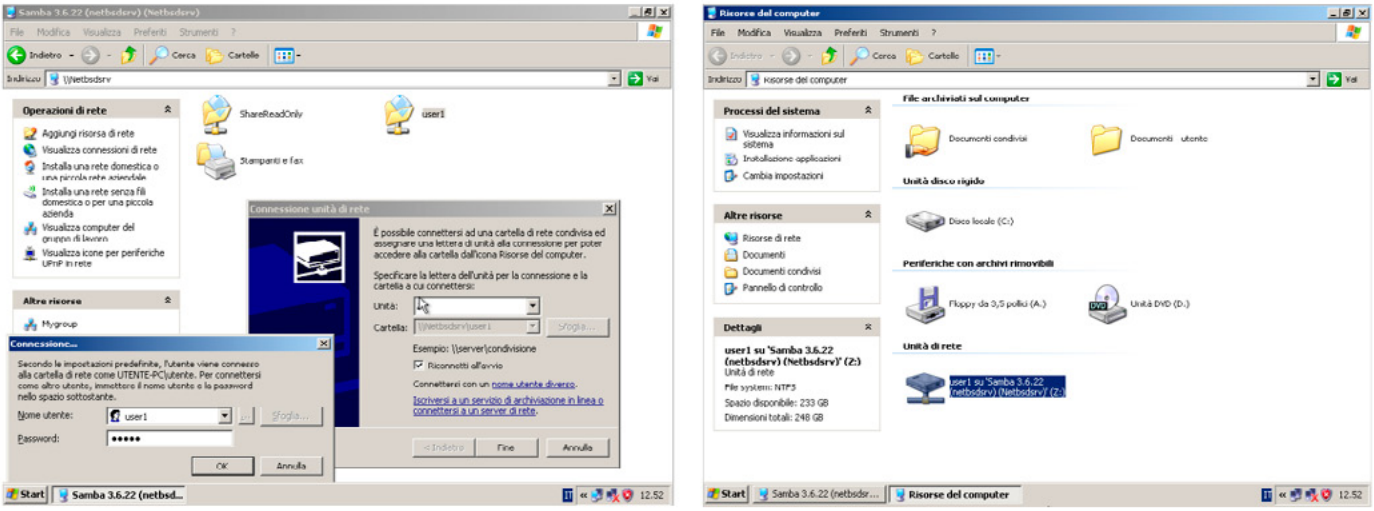
Errore durante l'eliminazione del file o della cartella

Impossibile eliminare file01: Accesso negato.

Controllare che il disco non sia pieno o protetto da scrittura e che il file non sia attualmente in uso.

OK

Figure 1. *a) Exploring CIFS Workgroups – b) Exploring read/write and read only shares*


Samba 3.6.22 (netbsdsrv) (Netbsdsrv)
\\Netbsdsrv
ShareReadOnly
user1
Stampanti e fax
Risorse del computer
File archiviati sul computer
Documenti condivisi
Documenti utente
Unità disco rigido
Disco locale (C:)
Periferiche con archivi rimovibili
Floppy da 3,5 pollici (A:)
Unità DVD (D:)
Unità di rete
user1 su 'Samba 3.6.22 (netbsdsrv) (Netbsdsrv)' (Z:)

Connessione unità di rete

È possibile connettersi ad una cartella di rete condivisa ed assegnare una lettera di unità alla connessione per poter accedere alla cartella dall'icona Risorse del computer.

Specificare la lettera dell'unità per la connessione e la cartella a cui connettersi:

Unità:

Cartella: \\Netbsdsrv\user1

Esempio: \\server\condivisione

☑ Riconnetti all'avvio

Connettersi con un nome utente diverso.

Iscriversi a un servizio di archiviazione in linea o connettersi a un server di rete.

< Indietro Fine Annulla

Connessione...

Secondo le impostazioni predefinite, l'utente viene connesso alla cartella di rete come UTENTE-PC\utente. Per connettersi come altro utente, immettere il nome utente e la password nello spazio sottostante.

Nome utente: user1

Password: •••••

OK Annulla

Dettagli

user1 su 'Samba 3.6.22 (netbsdsrv) (Netbsdsrv)' (Z:)
Unità di rete
File system: NTFS
Spazio disponibile: 233 GB
Dimensioni totali: 248 GB

Figure 2. *Mapping NetBSD Samba server Shares on Windows Clients*

Configuring an NFS server on NetBSD

In this section, we will use NFS to manage a shared folder `/usr/local/nfsshare` on the fileserver, which allows us to work on the same files from any computer on the network.

A small digression: NIS

NIS (Network Information Service), also known as “Yellow Pages Service”, or YP, is a directory management system very similar to LDAP and Microsoft Active Directory and is used to centralize the configuration files such as `/etc/hosts` and `/etc/passwd`. An example of the use of NIS is the centralization of accounts to have the same users on each host on the network without the hassle of sync files credentials.

It would be ideal to use a service like YP to ensure that all user IDs NFS/group are on the same server as the client. Otherwise, it will be necessary to maintain sync periodically.

To use NFS, make sure that the kernel has active support for the NFS share, both on the client and on the server. In particular, it will be necessary to uncomment or add the following lines in the file kernel:

```
file-system NFS   # Network File System client
```

the server must also have the following option:

```
options nfsserver    # Network File System server
```

NFS setup is very simple. The system manager has to simply enter all the directories that they want to export in `/etc/exports` file before starting the NFS daemon. In our example we have:

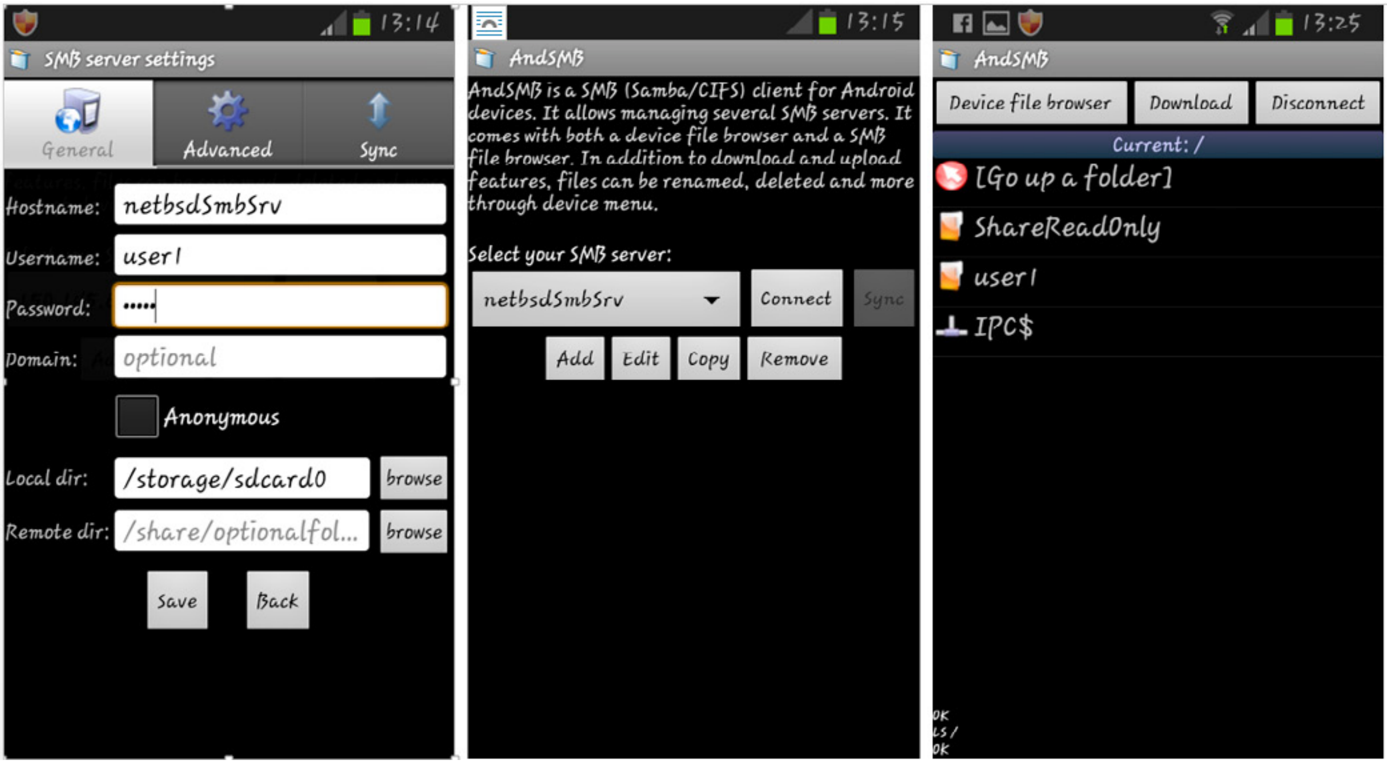
```
/usr/local/nfsshare -network 192.168.88.0 -mask
   255.255.0.0 -maproot = root
```

This will export the `/usr/local/nfsshare` folder on 192.168.88.x LAN only and is the required maproot line because otherwise the client will not have superuser root access. Now, start the daemons and NFS mount daemon (mountd and nfsd) as root on your server, in that order.

```
root@nfs-server# /etc/rc.d/rpcbind start
root@nfs-server# /etc/rc.d/mountd start
root@nfs-server# /etc/rc.d/nfsd start
root@nfs-server# /etc/rc.d/nfslocking start
```

To start NFS at server startup, you need to enter in the file `/etc/rc.conf`:

```
nfs_server=yes
rpcbind=yes
mountd=${nfs_server}
lockd=${nfs_server}
statd=${nfs_server}
```



Hostname: netbsdSmbSrv
Username: user1
Password: •••••
Domain: optional
□ Anonymous
Local dir: /storage/sdcard0
Remote dir: /share/optionalfol...

AndSMB is a SMB (Samba/CIFS) client for Android devices. It allows managing several SMB servers. It comes with both a device file browser and a SMB file browser. In addition to download and upload features, files can be renamed, deleted and more through device menu.

Select your SMB server: netbsdSmbSrv

Current: /
[Go up a folder]
ShareReadOnly
user1
IPC$

OK
LS /
OK

Figure 3. *Using NetBSD Samba server Shares on Android Clients*

To test the configuration, you can try to mount the folder from a client:

```
root@nfs-client # mount- t nfs nfs-server:/usr/local/
   nfsshare  /usr/local/nfsshare
```

If everything works correctly, just add all NFS volumes to be mounted automatically to `/etc/fstab` with lines similar to the following:

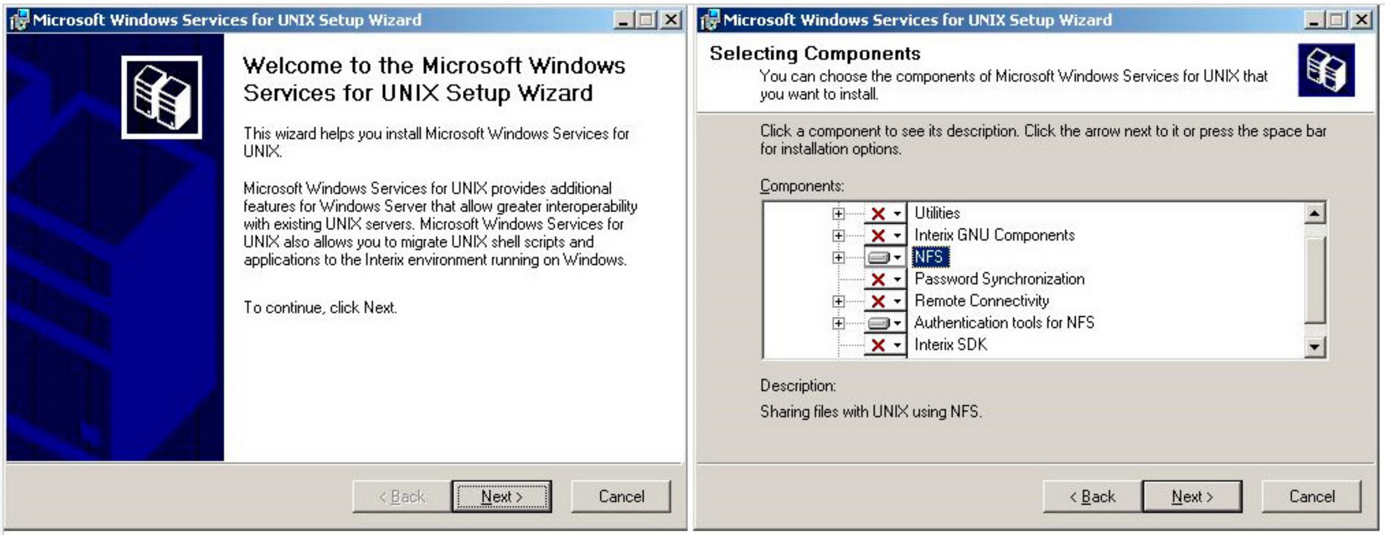
```
nfs-server:/usr/local/nfsshare
    /usr/local/nfsshare nfs rw
```

To map an NFS share in Windows exported from our NetBSD server, we can use the mount command, but first we need to install "NFS Client for Windows". If the client OS is Windows 7 Enterprise, Vista Enterprise, or Windows 2008, then the NFS Client setup can be done from the Add/Remove Software wizard in the Control Panel.

If the client OS is Windows 2000, Windows 2000 Service Pack 3, Windows 2000 Service Pack 4, Windows Server 2003 or Windows XP, then we must download the client from this URL: *http://www.microsoft.com/en-us/download/confirmation.aspx?id=274*.

If the required services are up and running on your client, you can now mount the NFS share from the command line using the mount command:

```
mount \\NetBsdNfsSrv\NfsShareFolder K:
```


Microsoft Windows Services for UNIX Setup Wizard
< Back
Next >
Cancel
Microsoft Windows Services for UNIX Setup Wizard
< Back
Next >
Cancel

Welcome to the Microsoft Windows Services for UNIX Setup Wizard

This wizard helps you install Microsoft Windows Services for UNIX.

Microsoft Windows Services for UNIX provides additional features for Windows Server that allow greater interoperability with existing UNIX servers. Microsoft Windows Services for UNIX also allows you to migrate UNIX shell scripts and applications to the Interix environment running on Windows.

To continue, click Next.

Selecting Components

You can choose the components of Microsoft Windows Services for UNIX that you want to install.

Click a component to see its description. Click the arrow next to it or press the space bar for installation options.

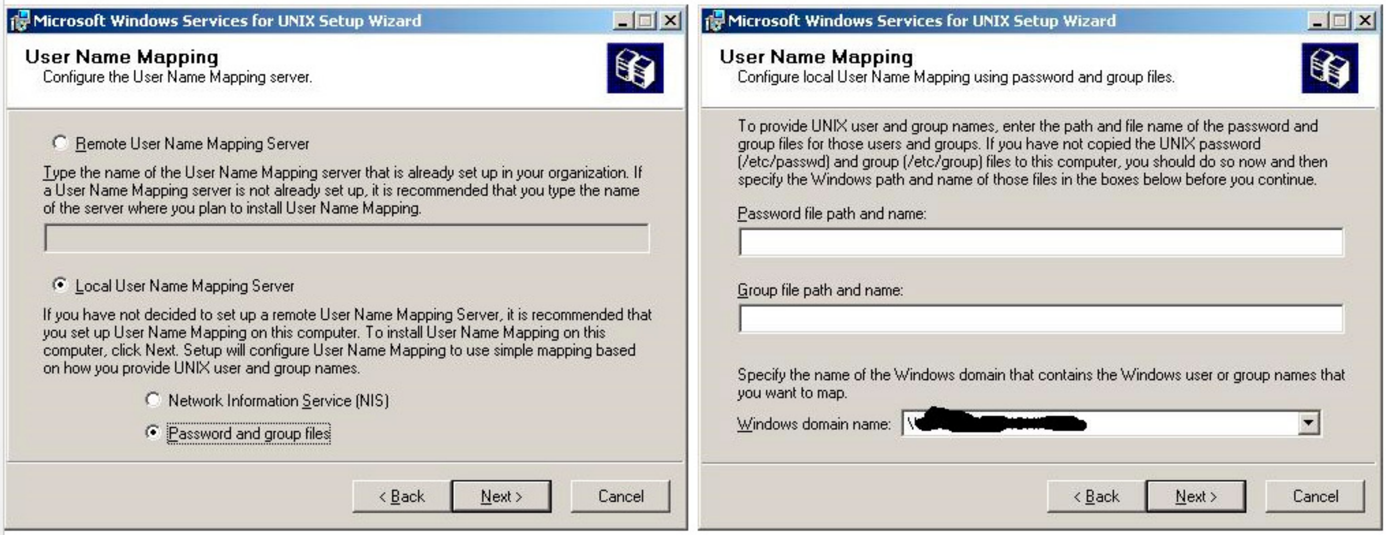
Components:

- ☒ Utilities
- ☒ Interix GNU Components
- NFS
- ☒ Password Synchronization
- ☒ Remote Connectivity
- Authentication tools for NFS
- ☒ Interix SDK

Description:

Sharing files with UNIX using NFS.

Figure 4. *Setup NSF Client/Server Services on Windows Clients (STEP 1)*


Microsoft Windows Services for UNIX Setup Wizard
< Back
Next >
Cancel
Microsoft Windows Services for UNIX Setup Wizard
< Back
Next >
Cancel

User Name Mapping

Configure the User Name Mapping server.

○ Remote User Name Mapping Server

Type the name of the User Name Mapping server that is already set up in your organization. If a User Name Mapping server is not already set up, it is recommended that you type the name of the server where you plan to install User Name Mapping.

● Local User Name Mapping Server

If you have not decided to set up a remote User Name Mapping Server, it is recommended that you set up User Name Mapping on this computer. To install User Name Mapping on this computer, click Next. Setup will configure User Name Mapping to use simple mapping based on how you provide UNIX user and group names.

○ Network Information Service (NIS)

● Password and group files

User Name Mapping

Configure local User Name Mapping using password and group files.

To provide UNIX user and group names, enter the path and file name of the password and group files for those users and groups. If you have not copied the UNIX password (/etc/passwd) and group (/etc/group) files to this computer, you should do so now and then specify the Windows path and name of those files in the boxes below before you continue.

Password file path and name:

Group file path and name:

Specify the name of the Windows domain that contains the Windows user or group names that you want to map.

Windows domain name: [redacted]

Figure 5. *Setup NSF Client/Server Services on Windows Clients (STEP 2)*

or by using the mapping resources wizard as shown for Samba shares. If NFS client services are not available in your OS (Windows 7 standard), you can use the Dokan library nfs client. Here is the setup procedure:

Download and install the Dokan library DokanInstall_X.X.X.exe, installing the Microsoft .NET Framework 4 first. Download and install Neko Drive NekoDrive_X_X_X.7z and launch the application, then change the Target Connection IP address to your server IP and set the version to V3 or V4.

By clicking on "connect", the client should login to our server and to mount the drive in windows, set the Device location and select a Disk name. Make sure Devices is set to the correct item (e.g. `\\NetBsdNfsSrv\NfsShareFolder`), and finally, by using the mount button, the drive should show up in Windows Explorer (Figure 5).

For Mac OS X clients users must open up the Disk Utility and choose File > NFS Mounts…

Next, they have to click the small plus (+) icon at the bottom and enter a valid NFS URL (IP + PATH), for example: `\\NetBsdNfsSrv\NfsShareFolder` and enter a Mount location (local mount), for example: `/Volumes/myNFS`, then they may optionally enable mounts as read-only and, at last, click Verify and OK. If everything went fine, they can open up Finder and browse to `/Volumes/myNFS`.

Configuring SSL with vsftpd

Vsftpd (Very Secure FTP Daemon) is an FTP server. It's lightweight, stable and secure for UNIX-like systems and is included in the official repositories, but to enable SSL support one must install it using pkgsrc:

```
# cd /usr/pkgsrc/net/vsftpd
```

Edit makefile to add support for SSL and then launch the installer:

```
# make install clean
```

Starting with vsftpd configuration, one must know that most of the settings in vsftpd are done by editing the file `/etc/vsftpd.conf`, which is well documented, so this section highlights only some important changes that you might want to perform. To enable the upload, a specific flag must be set to YES in `/etc/vsftpd.conf` in order to enable the changes to the file system:

```
write_enable = YES
```

You must set the following line in `/etc/vsftpd.conf` to allow users to members in `/etc/passwd` to access the system:

```
local_enable = YES
```

The following line in `/etc/vsftpd.conf` controls whether anonymous users can log in:

```
anonymous_enable = NO # Deny anonymous access
```

You can set up a chroot environment that prevents the user from leaving his home directory. To do this, add the following lines to `/etc/vsftpd.conf`:

```
chroot_list_enable = YES
chroot_list_file = /etc/vsftpd.chroot_list
```

The `chroot_list_file` variable specifies the file that contains directives for users to circumscribe. For an even more restrictive directive, you can specify the line:

```
chroot_local_user = YES
```

Listing 3. *A simple configuration file for vsftpd with SSL support*

```
# FTPES vsftpd.conf

listen=YES
anonymous_enable=NO
local_enable=YES
write_enable=YES
chroot_local_user=YES
chroot_list_enable=NO

# Turn on SSL
ssl_enable=YES
force_local_data_ssl=YES
force_local_logins_ssl=YES
ssl_tlsv1=YES
ssl_sslv2=YES
ssl_sslv3=YES
require_ssl_reuse=NO
ssl_ciphers=HIGH
rsa_cert_file=/etc/ssl/private/vsftpd.pem

#listen_port=990

#force_dot_files=YES
hide_ids=YES
max_per_ip=2
max_clients=20
```

In this way, local users will be limited by default, and the file specified by `chroot_list_file` lists the users that are not within the restricted chroot.

You can prevent users from accessing the FTP server with the addition of two lines in `/etc/vsftpd.conf`:

```
userlist_enable = YES
userlist_file = / etc / vsftpd.user_list
```

`userlist_file` now specifies the file that lists users who are not authorized to log in. If you want to restrict access only to certain users, add the line:

```
userlist_deny = NO
```

The file specified by `userlist_file` now contains the users who are allowed to login.

You can limit the data transfer rate, and the number of client connections per IP and local user by adding the information in `/etc/vsftpd.conf`:

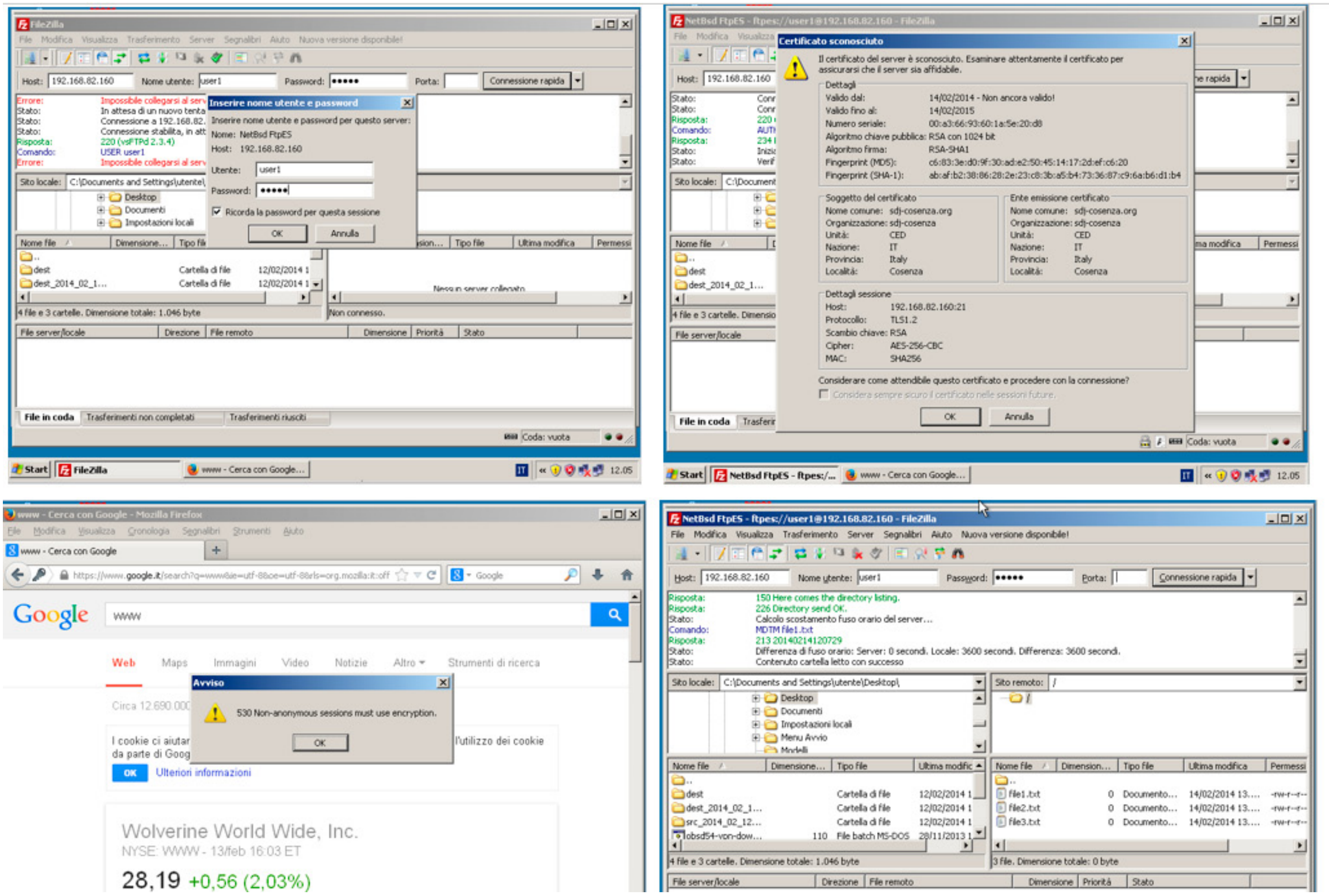
```
local_max_rate = 1000000 # Maximum data transfer rate in
    bytes per second
max_clients = 50 # Maximum number of clients that can
    be connected
max_per_ip = 2 # Maximum number of connections per IP
```

Using vsftpd in standalone mode, or via inetd

```
#listen = YES  # executable in stand-alone mode
listen = NO #  executable in inetd mode
```

To use SSL for the security of FTP, you need to generate an SSL certificate as follows:

```
# cd /etc/ssl/private
# openssl req -x509 -nodes -days 7300 -newkey rsa:2048 –
    keyout \\ /etc/ssl/private/vsftpd.pem -out /etc/ssl/
    private/vsftpd.pem
# chmod 600 /etc/ssl/private/vsftpd.pem
```



Host: 192.168.82.160 Nome utente: user1 Password: ••••• Porta:

```
Errore:     Impossibile collegarsi al serv
Stato:      In attesa di un nuovo tenta
Stato:      Connessione a 192.168.82.
Stato:      Connessione stabilita, in att
Risposta:   220 (vsFTPd 2.3.4)
Comando:    USER user1
Errore:     Impossibile collegarsi al serv
```

Inserire nome utente e password

Inserire nome utente e password per questo server:
Nome: NetBsd FtpES
Host: 192.168.82.160
Utente: user1
Password: •••••
☑ Ricorda la password per questa sessione

Sito locale: C:\Documents and Settings\utente\

Nome file	Dimensione...	Tipo file	Ultima modifica
..			
dest		Cartella di file	12/02/2014 1
dest_2014_02_1...		Cartella di file	12/02/2014 1

4 file e 3 cartelle. Dimensione totale: 1.046 byte

Nessun server collegato

Non connesso.

NetBsd FtpES - ftpes://user1@192.168.82.160 - FileZilla

Certificato sconosciuto

Il certificato del server è sconosciuto. Esaminare attentamente il certificato per assicurarsi che il server sia affidabile.

Dettagli

Valido dal:	14/02/2014 - Non ancora valido!
Valido fino al:	14/02/2015
Numero seriale:	00:a3:66:93:60:1a:5e:20:d8
Algoritmo chiave pubblica:	RSA con 1024 bit
Algoritmo firma:	RSA-SHA1
Fingerprint (MD5):	c6:83:3e:d0:9f:30:ad:e2:50:45:14:17:2d:ef:c6:20
Fingerprint (SHA-1):	ab:af:b2:38:86:28:2e:23:c8:3b:a5:b4:73:36:87:c9:6a:b6:d1:b4

Soggetto del certificato

Nome comune:	sdj-cosenza.org
Organizzazione:	sdj-cosenza
Unità:	CED
Nazione:	IT
Provincia:	Italy
Località:	Cosenza

Ente emissione certificato

Nome comune:	sdj-cosenza.org
Organizzazione:	sdj-cosenza
Unità:	CED
Nazione:	IT
Provincia:	Italy
Località:	Cosenza

Dettagli sessione

Host:	192.168.82.160:21
Protocollo:	TLS1.2
Scambio chiave:	RSA
Cipher:	AES-256-CBC
MAC:	SHA256

Considerare come attendibile questo certificato e procedere con la connessione?
□ Considera sempre sicuro il certificato nelle sessioni future.

www - Cerca con Google - Mozilla Firefox

Avviso

530 Non-anonymous sessions must use encryption.

Wolverine World Wide, Inc.
NYSE: WWW - 13/feb 16:03 ET
28,19 +0,56 (2,03%)

NetBsd FtpES - ftpes://user1@192.168.82.160 - FileZilla

Host: 192.168.82.160 Nome utente: user1 Password: ••••• Porta:

```
Risposta:   150 Here comes the directory listing.
Risposta:   226 Directory send OK.
Stato:      Calcolo scostamento fuso orario del server...
Comando:    MDTM file1.txt
Risposta:   213 20140214120729
Stato:      Differenza di fuso orario: Server: 0 secondi. Locale: 3600 secondi. Differenza: 3600 secondi.
Stato:      Contenuto cartella letto con successo
```

Sito locale: C:\Documents and Settings\utente\Desktop\ Sito remoto: /

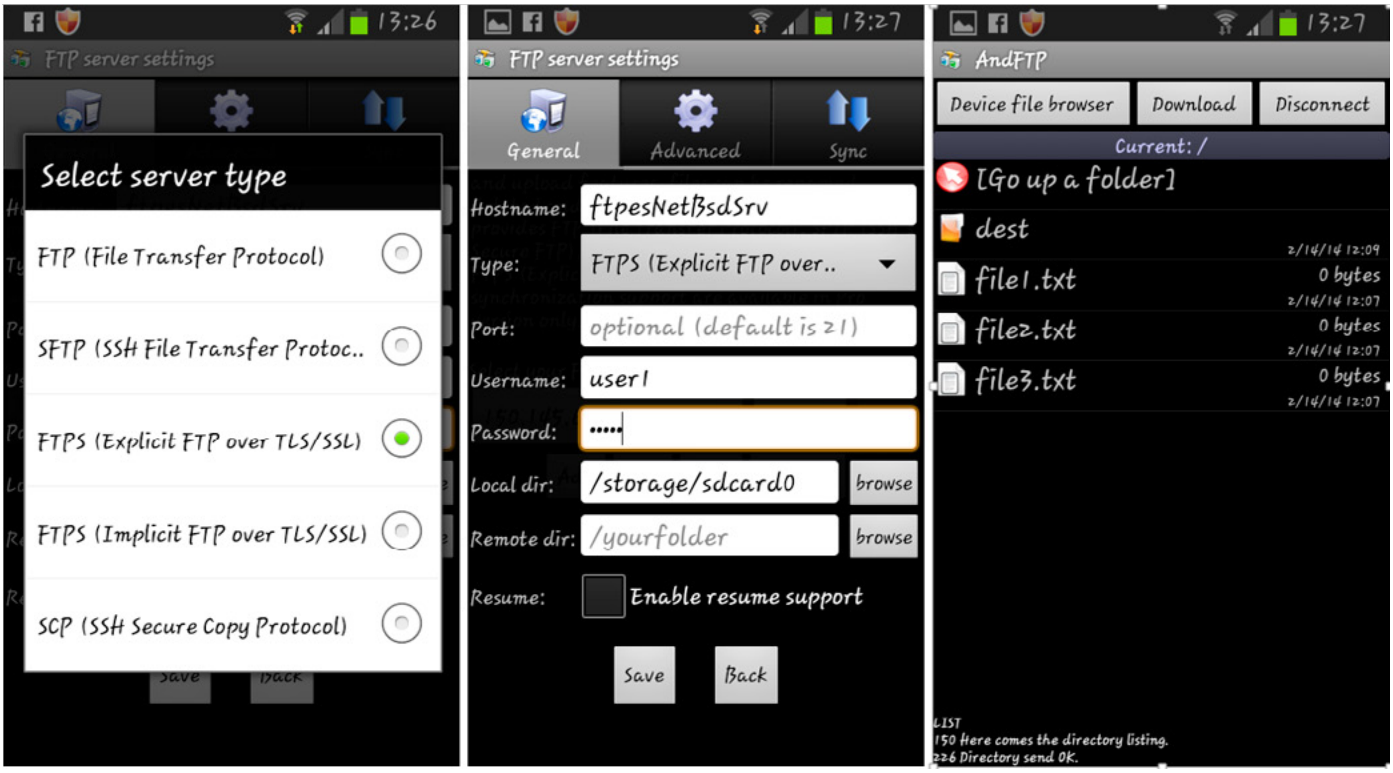
Nome file	Dimensione...	Tipo file	Ultima modific
..			
dest		Cartella di file	12/02/2014 1
dest_2014_02_1...		Cartella di file	12/02/2014 1
src_2014_02_12...		Cartella di file	12/02/2014 1
obsd54-vpn-dow...	110	File batch MS-DOS	28/11/2013 1

4 file e 3 cartelle. Dimensione totale: 1.046 byte

Nome file	Dimension...	Tipo file	Ultima modifica	Permessi
..				
file1.txt	0	Documento...	14/02/2014 13....	-rw-r--r--
file2.txt	0	Documento...	14/02/2014 13....	-rw-r--r--
file3.txt	0	Documento...	14/02/2014 13....	-rw-r--r--

3 file. Dimensione totale: 0 byte

Figure 6. *Setup FTPES Client (Filezilla) on Windows (also works in Linux and Mac OSX)*



Select server type

FTP (File Transfer Protocol) ○

SFTP (SSH File Transfer Protoc.. ○

FTPS (Explicit FTP over TLS/SSL) ●

FTPS (Implicit FTP over TLS/SSL) ○

SCP (SSH Secure Copy Protocol) ○

Hostname: ftpesNetBsdSrv

Type: FTPS (Explicit FTP over..

Port: optional (default is 21)

Username: user1

Password: •••••

Local dir: /storage/sdcard0 browse

Remote dir: /yourfolder browse

Resume: □ Enable resume support

Current: /

[Go up a folder]

dest 2/14/14 12:09

file1.txt 0 bytes 2/14/14 12:07

file2.txt 0 bytes 2/14/14 12:07

file3.txt 0 bytes 2/14/14 12:07

```
LIST
150 Here comes the directory listing.
226 Directory send OK.
```

Figure 7. *Setup FTPES Client (AndFTP) on Android clients*

The server will conduct you through a series of questions about the company and since it is expected to have to be used with guarantees of trust (trusted), it will be better to get one from companies like Symantec and Verisign (Listing 3).

To test the setup, you have to add the following lines to `/etc/rc.conf`:

```
vsftpd=YES
```

and then start the service with:

```
root@ftps-server# /etc/rc.d/vsftpd start
```

Finally, try to connect with a client that can handle FTP, such as Filezilla (Figure 6).

If everything works correctly, you will be prompted to accept the certificate and then you can access your files (see Figure 7).

As shown with samba, it's possible to use android phones to connect our secure FTP service.

Conclusion

A file server is an important service in networks of any size. Today, there are many cloud services like Dropbox and Google Drive, but for confidentiality reasons, a company may not want to entrust their data to others. So it is essential to be able to rely on cross-platform and robust file sharing services. In this article, we wanted to focus on three of the most commonly used: FTP over SSL, Samba/CIFS and NFS, and compare and contrast their strengths and weaknesses. It is the responsibility of the network administrator to consider the technology best suited to the needs of the company from time to time, in order to obtain the best compromise between performance and security.

ANTONIO FRANCESCO GENTILE

Antonio Francesco Gentile lives in Calabria, Italy. He is a network and software engineer. He works as a network manager at ICAR CNR (National Research Center) with the "Culture Lab" (http://culture.deis.unical.it), the Department of Telematics at the University of Calabria, the computer science associations "Hacklab Cosenza" (http://hacklab.cosenzainrete.it/) and "Verde Binario" (http://www.verdebinario.org/) and is a freelance columnist for Italian magazines "Linux & C" (http://www.oltrelinux.com/) and "Linux Magazine" (http://www.linuxmagazine.it/).

Dr.WEB®
since 1992
ERA Dr.Web
Emergency Response Anti-virus

DragonFlyBSD Part-1

As Backup servers in HIFX (hifx.co.in)

DragonFlyBSD, the fork of FreeBSD by founder Matthew Dillon with the long-term goal of providing transparent single system image clustering, supports both the IA-32 & AMD64 platforms. Previously including pkgsrc from the NetBSD project as the package management system, it has recently switched to native Dports, DragonFly's own third-party software build system, based on FreeBSD's Ports Collection.

What you will learn…

- How HIFX (hifx.co.in) uses DragonFly as its backup servers

What you should know…

- Basic admin skills

This article by the grace of God endeavours to describe how HIFX (hifx.co.in) uses DragonFly for its backup servers, leveraging the features of its HAMMER1 file systems; namely remote mirroring, snapshots, pruning, and dedup in two particular use cases.

The Reasons HIFX uses Dragonfly as its Backup Server are

Rolling release – by following the development version

Development branch is stable enough for most cases. If I keep an eye on the [Heads UP] mails sent to the DragonFly users list I can avoid trouble. There is no need for major upgrades every six months; I just upgrade little by little weekly or monthly as I have time.

2 500GB disks but no fsck after unclean shutdown

The hammer file system is designed to work without fscks. When working with large disks, this is a major time saver after a crash or unclean shut down.

Sufficient Redundancy using 'hammer remote mirroring' without RAID parity checks

HAMMER allows to create PFSes (Pseudo File Systems) inside Mother File system which acts as a fully mountable file system. PFSes can be created in two modes: Master & Slave. Each PFS has a "unique-uuid" and a "shared-uuid". If the shared-uuid of a Master PFS and a Slave PFS are the same then mirroring (replication) is possible between them. The Master and Slave can be on two different machines thousands of miles apart but connected through the network. Reboots of machines hosting either Slave PFS or Master PFS resumes the replication immediately without long parity checks like that of a RAID system. This simplifies offsite backups very much.

Instant (every 5 mins) backup for Windows/Mac OS X/BSD/Linux/Solaris users

Just drag and drop the files you need from backup. All you need is an SMB client. You could share the backup files using NFS or any other sharing mechanism too.

This use case includes developers working on small projects which last only a month or a bit longer. This type of set up will be apt for many organizations which make developments on small projects without the use of any version control system like Git, Mercurial, Subversion or MS VSS. The environment features and backup mechanism typically are:

- On the development server each project is a Samba share in `/var/www` on a BSD/OS X/Linux system, with typically Apache/Nginx as a web server and MySQL/PostgreSQL as database.

- On the DragonFly backup server a master PFS is created with the command

```
mkdir /pfs/www5mBak && hammer pfs-master /pfs/www5mBak/
www-hot
```

- Every 5 minutes changes from `/var/www` from the development server are rsynced with the master PFS on the backup server and a snapshot is taken using the following cron entry in the DragonFly Server

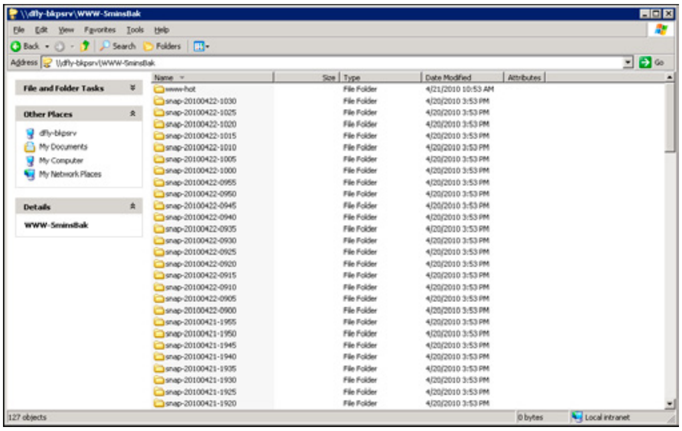
```
*/5 * * * * /usr/pkg/bin/rsync -az --delete root@
development-server:/var/www/ root@dragonfly-server-ip:/
pfs/www5mBak/www-hot/ && hammer snapshot /pfs/www5mbak/
www-hot /pfs/www5mBak "rsync"
```

- On the DragonFly backup server `/pfs/www5mBak` is shared using Samba for developers running MAC OS X, BSDs, Linux & MS Windows, who can easily browse project files every five minutes. From a Windows Explorer the backup Samba share on DragonFLY will look like Figure 1.

The developers can browse the folder for a particular time for a particular file(s) backup and drag and drop it to the development environment. Each snapshot will have the complete set of files and not just the diffs. We also serve mysql backups every hour in the following way.

The Master PFSes in one DragonFly server are mirrored to a slave PFS in another Dragonfly server at a remote location through the network using ssh.

This part was the greatest success in the company among developers. They have become very relaxed about backups now.



Name	Size	Type	Date Modified	Attributes
www-hot		File Folder	4/21/2010 10:53 AM	
snap-20100422-1030		File Folder	4/20/2010 3:53 PM	
snap-20100422-1025		File Folder	4/20/2010 3:53 PM	
snap-20100422-1020		File Folder	4/20/2010 3:53 PM	
snap-20100422-1015		File Folder	4/20/2010 3:53 PM	
snap-20100422-1010		File Folder	4/20/2010 3:53 PM	
snap-20100422-1005		File Folder	4/20/2010 3:53 PM	
snap-20100422-1000		File Folder	4/20/2010 3:53 PM	
snap-20100422-0955		File Folder	4/20/2010 3:53 PM	
snap-20100422-0950		File Folder	4/20/2010 3:53 PM	
snap-20100422-0945		File Folder	4/20/2010 3:53 PM	
snap-20100422-0940		File Folder	4/20/2010 3:53 PM	
snap-20100422-0935		File Folder	4/20/2010 3:53 PM	
snap-20100422-0930		File Folder	4/20/2010 3:53 PM	
snap-20100422-0925		File Folder	4/20/2010 3:53 PM	
snap-20100422-0920		File Folder	4/20/2010 3:53 PM	
snap-20100422-0915		File Folder	4/20/2010 3:53 PM	
snap-20100422-0910		File Folder	4/20/2010 3:53 PM	
snap-20100422-0905		File Folder	4/20/2010 3:53 PM	
snap-20100422-0900		File Folder	4/20/2010 3:53 PM	
snap-20100421-1955		File Folder	4/20/2010 3:53 PM	
snap-20100421-1950		File Folder	4/20/2010 3:53 PM	
snap-20100421-1945		File Folder	4/20/2010 3:53 PM	
snap-20100421-1940		File Folder	4/20/2010 3:53 PM	
snap-20100421-1935		File Folder	4/20/2010 3:53 PM	
snap-20100421-1930		File Folder	4/20/2010 3:53 PM	
snap-20100421-1925		File Folder	4/20/2010 3:53 PM	
snap-20100421-1920		File Folder	4/20/2010 3:53 PM	

127 objects | 0 bytes | Local intranet

Figure 1. *The backup Samba share on Dragon-FLY*

Automated daily backup of Linux LXC virtual servers with optimised storage space

Another use case is to backup LXC containers to HAMMER PFS. In our Linux servers LXC containers reside in a logical volume. We take the snapshot of the logical volumes with LXC containers and rsync from the LVM snapshot to the hammer file system and create a hammer snapshot. Thus if a linux server with LXC volume crashes it is only a matter of rsyncing back the LXC containers to the new server's logical volume.

De-dup helps in saving space; de-duplication implemented in HAMMER helps save storage space of backups

Currently we get a de-dup ratio from 4.01 to 13.78 depending on the type of file backed up. A ratio of 13.78 for us means 117 GB data is referenced while only 8747 MB data is allocated. It is like storing 117 GB of data in 8.7 GB space.

- *http://leaf.dragonflybsd.org/mailarchive/users/2011-07/msg00023.html*
- *http://dragonflybsd-os.blogspot.in/*

Variable File System Snapshot Schemes for Master and Slave PFSes

Snapshots of a file system at a particular time show how that file system looked at that time. It is possible to configure different snapshotting schemes for the master and the slave. The Master may be snapshotted every 5 minutes whereas the slave may be snapshotted every one hour. Also the state of the filesystem can be accessed live at 30-60 second boundaries without having to make explicit snapshots, up to a configurable fine-grained retention time.

Remote Encrypted File System Mirroring using "hammer mirror-stream" & SSH

Data passes from HAMMER PFS Master to a remote HAMMER PFS slave through ssh continuously and when there is a change is master if you use "hammer mirror-stream". Since the data passes through ssh there is no need to configure further security measures for the data in transit.

Able to Add Volumes to Hammer File System on the Fly

If a HAMMER volume is full then other disks can be added to it like the Linux LVM to increase its capacity.

SIJU GEORGE

Siju George is Senior Systems Administrator at HIFX IT & Media Services Private Limited. Experienced in Systems Administration on OpenBSD, FreeBSD, DragonFlyBSD, Debian, Redhat and other flavors of Linux, Mac OS X and Microsoft Technologies since 2002.

Getting to Grips with the Gimp – Part 2

In our new series on image manipulation and design, we will continue to look at graphic design basics, and how to use the most popular Open Source graphics software – The Gimp.

What you will learn…

- How to manipulate images like a design pro

What you should know…

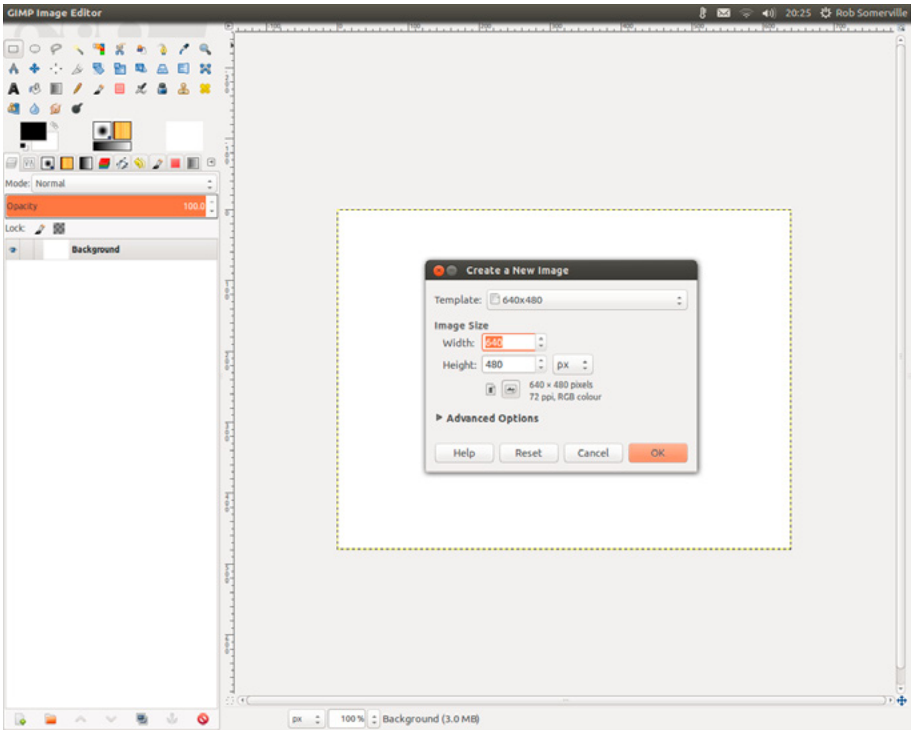
- General PC administration skills

The gimp is great.

In the last article we looked at the basics of The Gimp and created a rose with a reflection. In this tutorial, we will look further at layers, gradients, light, text and shadow and create the image “The gimp is great”.

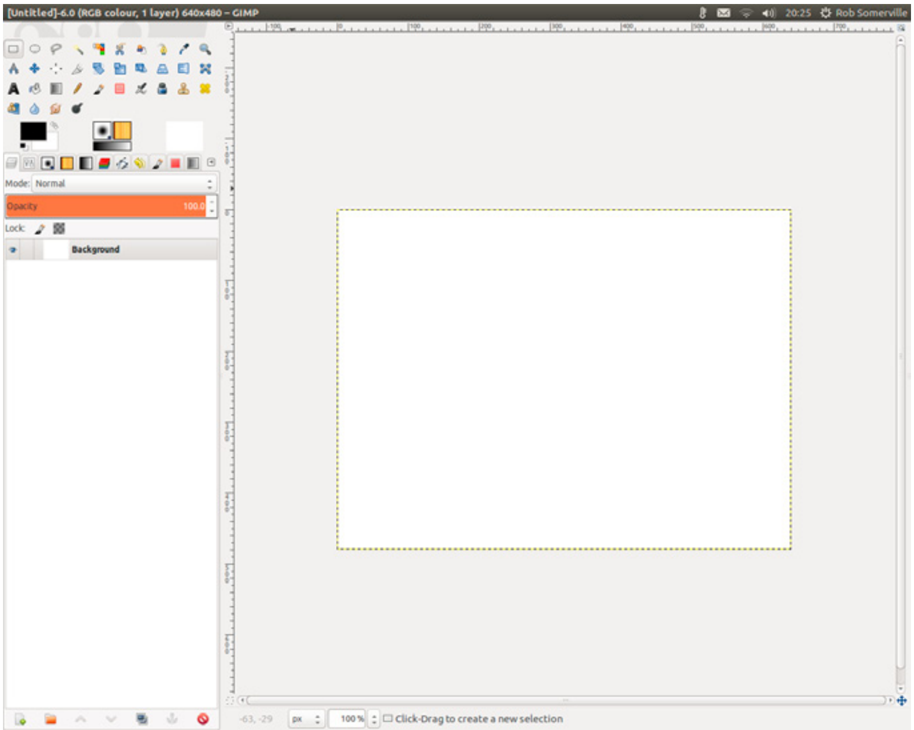
Step 1

From File → new (or Ctrl N) create a new 640 x 480 image using the 640 x 480 template [Figure 1 – 2].



Template: 640x480
Width: 640
Height: 480 px
640 × 480 pixels
72 ppi, RGB colour
px 100 % Background (3.0 MB)

Figure 1. *Create a new image*

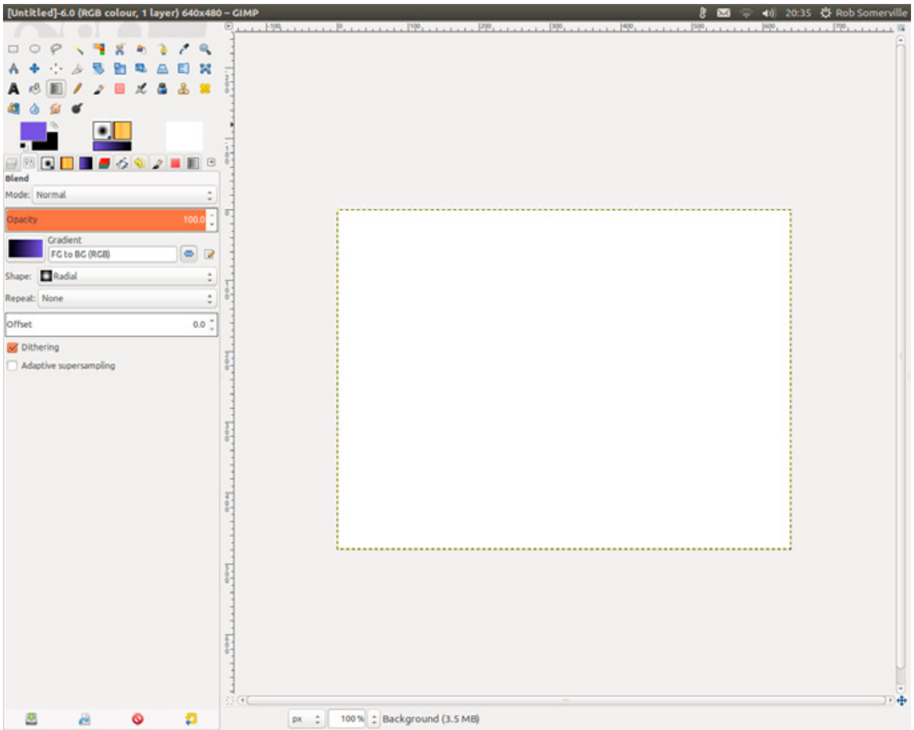


-63, -29 px 100 % Click-Drag to create a new selection

Figure 2. *Our 640 x 480 canvas*

Step 2

Pick a light foreground colour and a light background colour. I have used 6e53e0 for the foreground and 000000 (Black) for the background [Figure 3].



[Untitled]-6.0 (RGB colour, 1 layer) 640x480 – GIMP

Blend

Mode: Normal

Opacity 100.0

Gradient FG to BG (RGB)

Shape: Radial

Repeat: None

Offset 0.0

☑ Dithering

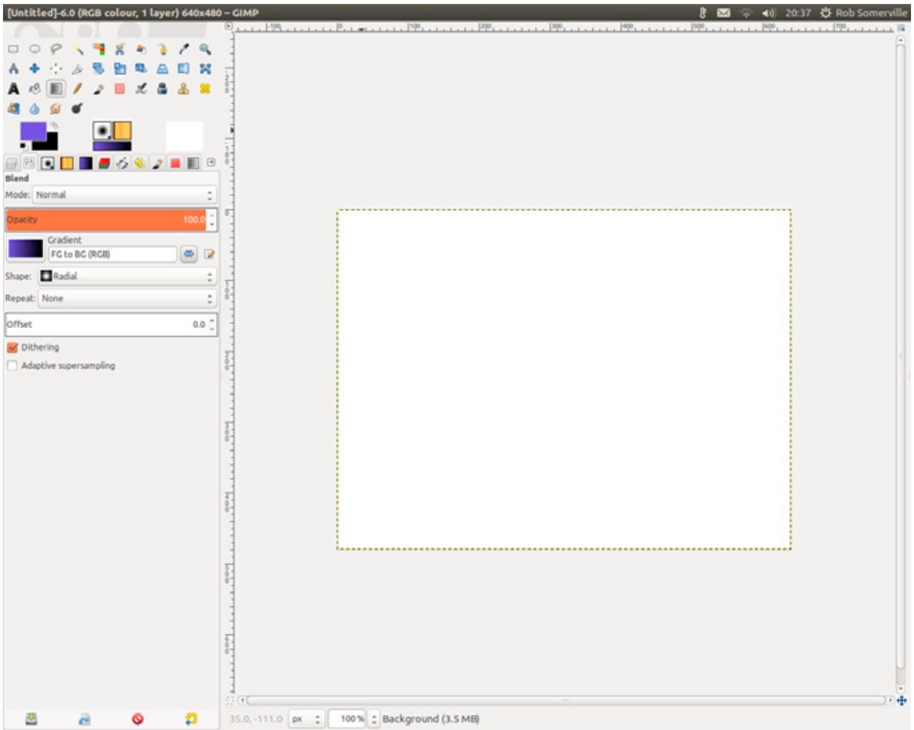
□ Adaptive supersampling

px 100 % Background (3.5 MB)

Figure 3. *Select colours and gradient mode*

Step 3

Select the Blend tool with a radial shape. Ensure the gradient is FG to BG RGB [Figure 4].



[Untitled]-6.0 (RGB colour, 1 layer) 640x480 – GIMP

Blend

Mode: Normal

Opacity 100.0

Gradient FG to BG (RGB)

Shape: Radial

Repeat: None

Offset 0.0

☑ Dithering

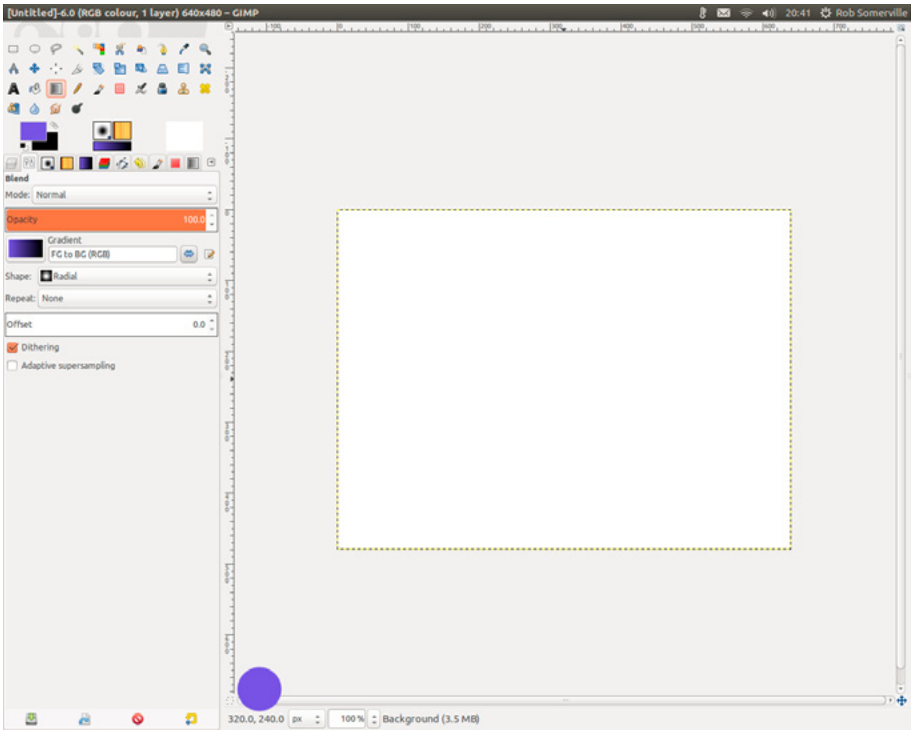
□ Adaptive supersampling

35.0, -111.0 px 100 % Background (3.5 MB)

Figure 4. *Changing the gradient direction with the gradient arrows*

Step 4

Move the cursor to half the foreground and height of the image (320 x 240). Click on the middle of the screen, press Ctrl to constrain the angle to 45 degrees, and drag to the bottom edge of the image. This will create a graduated background [Figure 5 – 6].

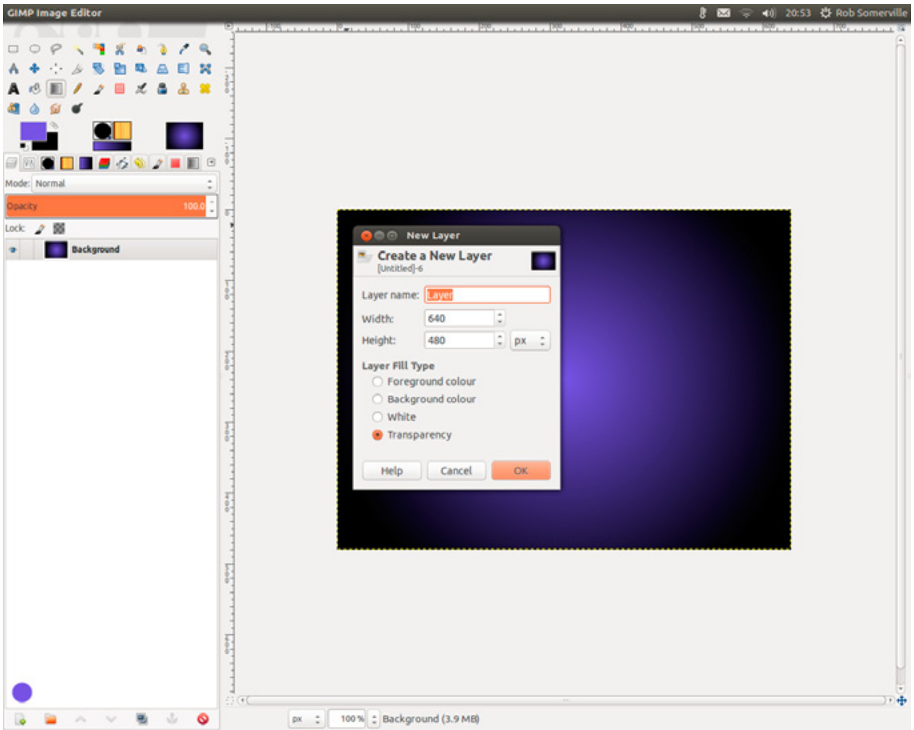


[Untitled]-6.0 (RGB colour, 1 layer) 640x480 – GIMP

Blend
Mode: Normal
Opacity 100.0
Gradient FG to BG (RGB)
Shape: Radial
Repeat: None
Offset 0.0
☑ Dithering
□ Adaptive supersampling

320.0, 240.0 px 100 % Background (3.5 MB)

Figure 5. *Using the position indicator to move cursor to the centre of the image*



GIMP Image Editor

Mode: Normal
Opacity 100.0
Lock:
Background

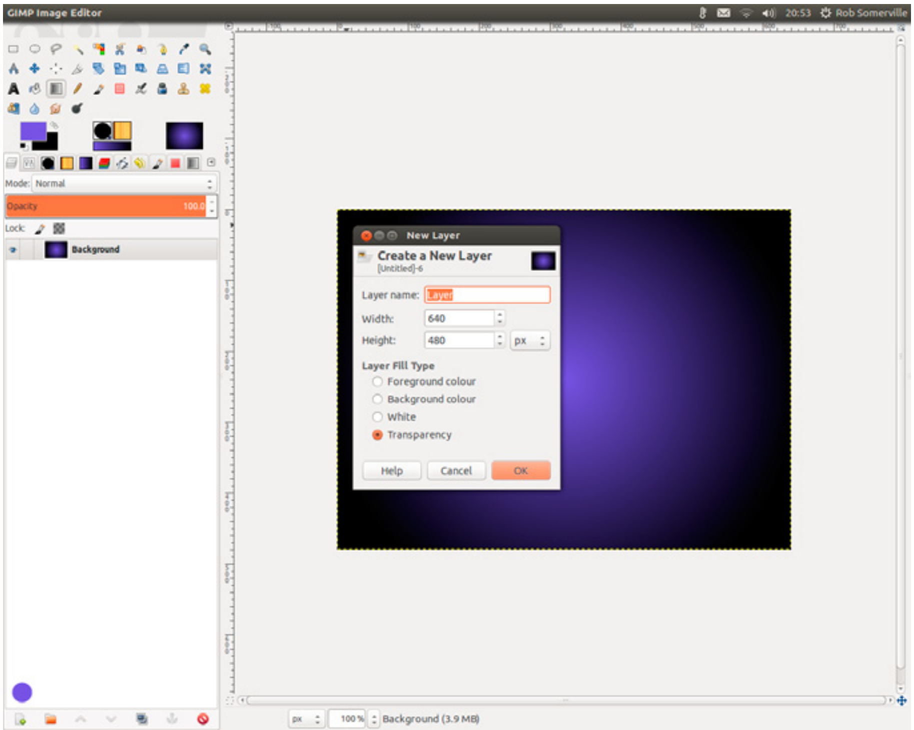
New Layer
Create a New Layer
[Untitled]-6
Layer name: Layer
Width: 640
Height: 480 px
Layer Fill Type
○ Foreground colour
○ Background colour
○ White
● Transparency

px 100 % Background (3.9 MB)

Figure 6. *The background gradient*

Step 5

Click back onto the layers tab and create a new transparent layer. Either right click in the layers area or click on the New layer icon [Figure 7].



GIMP Image Editor

Mode: Normal

Opacity 100.0

Lock:

Background

New Layer

Create a New Layer
[Untitled]-6

Layer name: Layer

Width: 640

Height: 480 px

Layer Fill Type

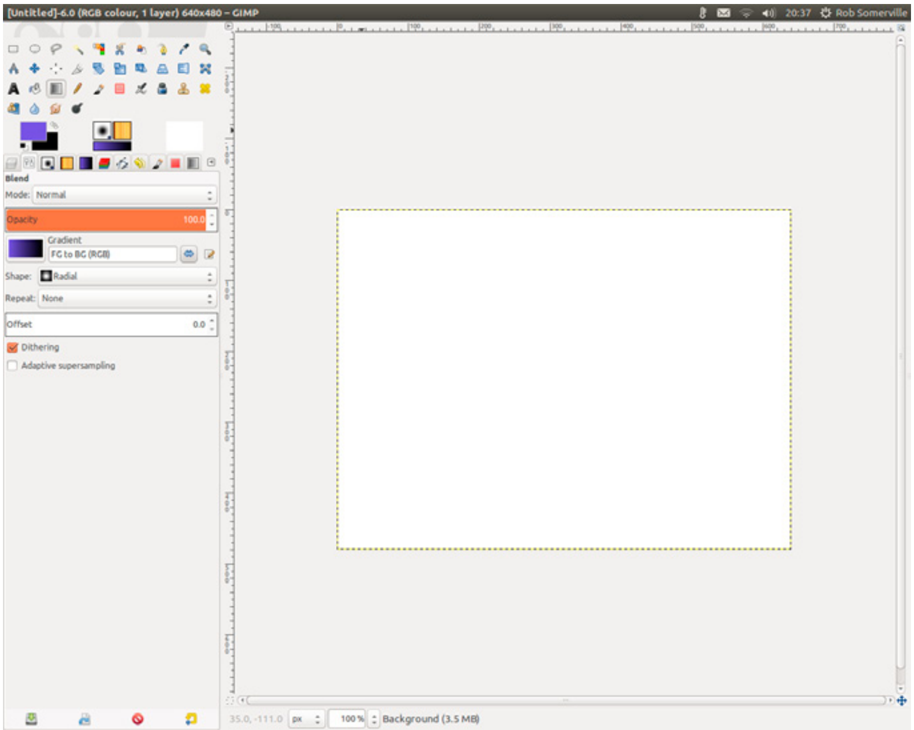
○ Foreground colour
○ Background colour
○ White
● Transparency

px 100 % Background (3.9 MB)

Figure 7. *Adding a new layer*

Step 6

Using the text tool, click and drag an area in the middle of the screen and add the text “The gimp is great.” Highlight the text, and change the font size, character spacing and colour so that a new text layer is created. Don’t worry about the exact position, as we can adjust this later. We will now have three layers as the text tool automatically creates a new layer [Figure 8].



[Untitled]-6.0 (RGB colour, 1 layer) 640x480 – GIMP

Blend

Mode: Normal

Opacity 100.0

Gradient FG to BG (RGB)

Shape: Radial

Repeat: None

Offset 0.0

☑ Dithering
□ Adaptive supersampling

35.0, -111.0 px 100 % Background (3.5 MB)

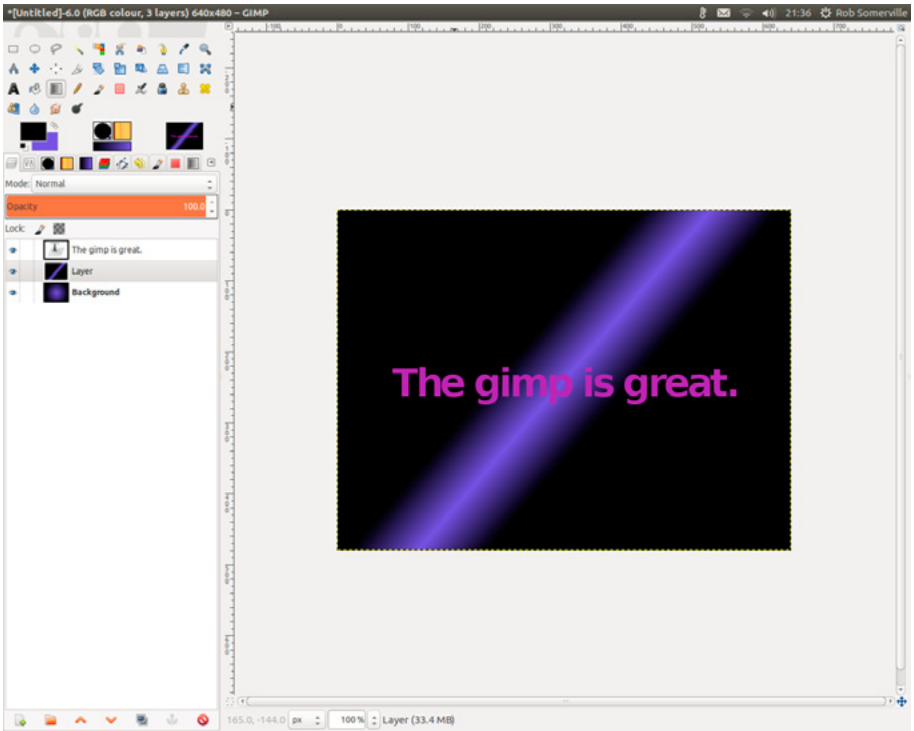
Figure 8. *Adding text*

Step 7

Click on the text layer and then on the move tool and align the middle of the centre of the “p” in “gimp” so that the brightest area of the gradient shines through.

Step 8

Click on the transparent layer we made earlier. Reverse the background and foreground colour by clicking on the small arrow between the foreground and background. Click on the gradient tool and change the fill to Bi-Linear. Click inside the “p” and drag at 45 degrees just below the text area. Ensure the darker colour is on the right hand side of the gradient [Figure 9].


*[Untitled]-6.0 (RGB colour, 3 layers) 640x480 – GIMP

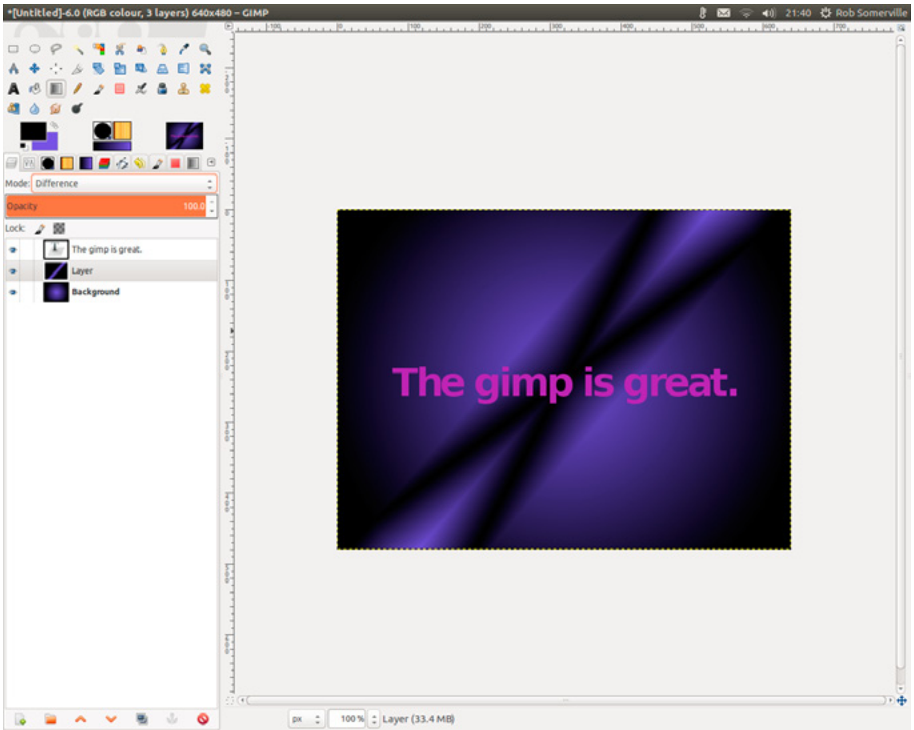
Mode: Normal

Opacity 100.0

Figure 9. *Adding another layer*

Step 9

Click on the layers tab and then on the mode dropdown. Scroll through the options and choose the effect you like best. I have used the difference mode [Figure 10].


*[Untitled]-6.0 (RGB colour, 3 layers) 640x480 – GIMP

Mode: Difference

Opacity 100.0

Figure 10. *The merged layers (Difference)*

Step 10

Click back onto the text layer and right click on the layer choosing Alpha to selection to select the text. Add a new transparent layer and click on it [Figure 11].

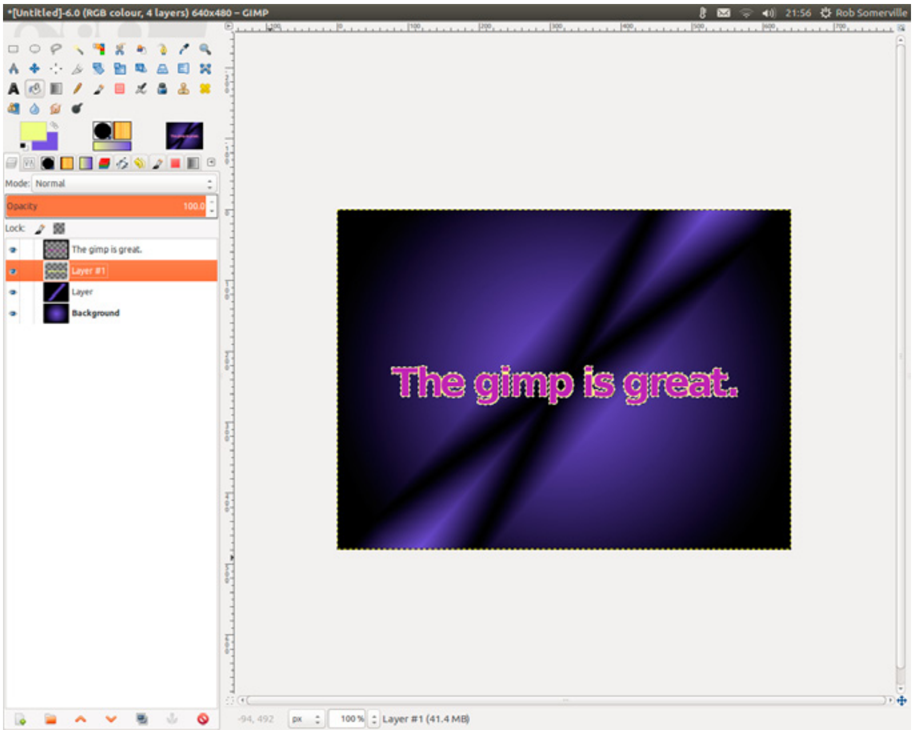


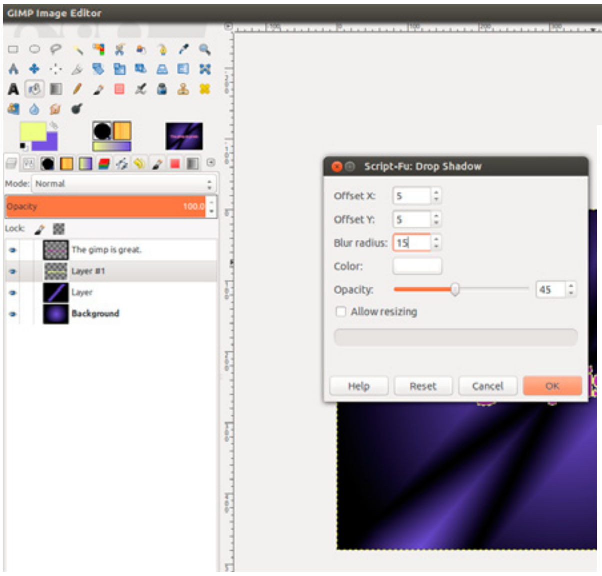
Figure 11. *Alpha selection grown with yellow outline*

Step 11

Pick a vibrant foreground colour, and click on Select → Grow and grow the outline by 2px. Press Ctrl, to fill with your chosen colour. Drag the layer below the text layer.

Step 12

Select Filters → Light and Shadow → Drop shadow and create a 45 percent opacity drop shadow in white. Hide the shadow layer [Figure 12 – 13].



Script-Fu: Drop Shadow

Offset X: 5

Offset Y: 5

Blur radius: 15

Color:

Opacity: 45

□ Allow resizing

Figure 12. *Blurring the drop shadow*

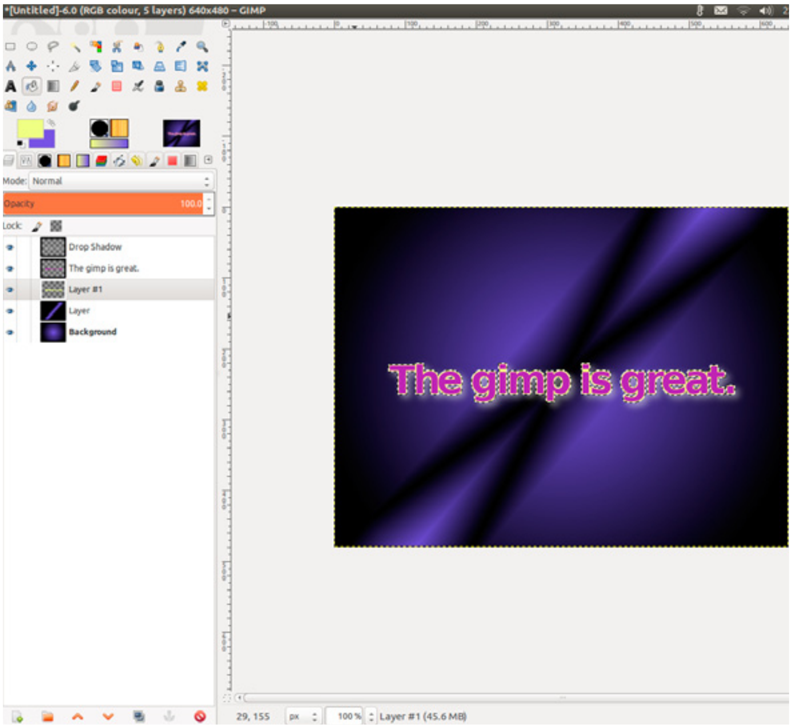
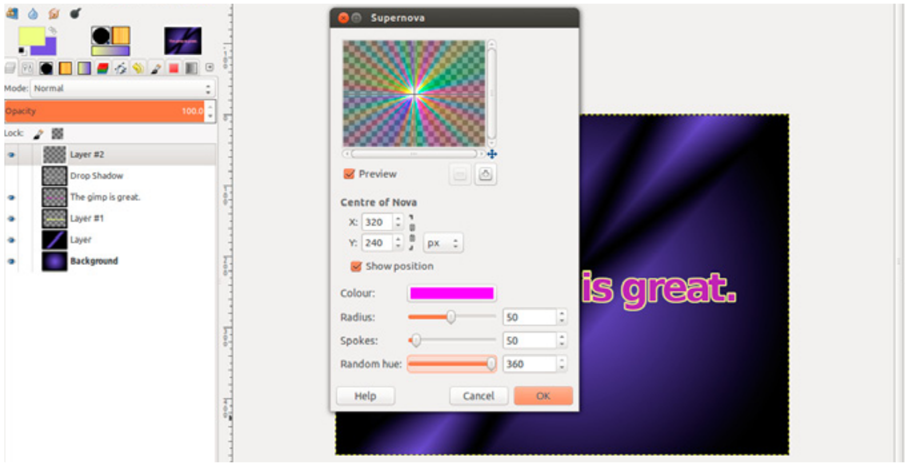


Figure 13. *Drop shadow in place*

Step 13

Create a new transparent layer and ensure it is enabled. Select Filters → Light and Shadow → Supernova and create a vibrant pink flare at position 320 x 240 with Radius and Spokes 50 and maximum hue [Figure 14 – 15].


Supernova

☑ Preview

Centre of Nova

X: 320

Y: 240

px

☑ Show position

Colour:

Radius: 50

Spokes: 50

Random hue: 360

Figure 14. *Adding a multi-hue supernova*

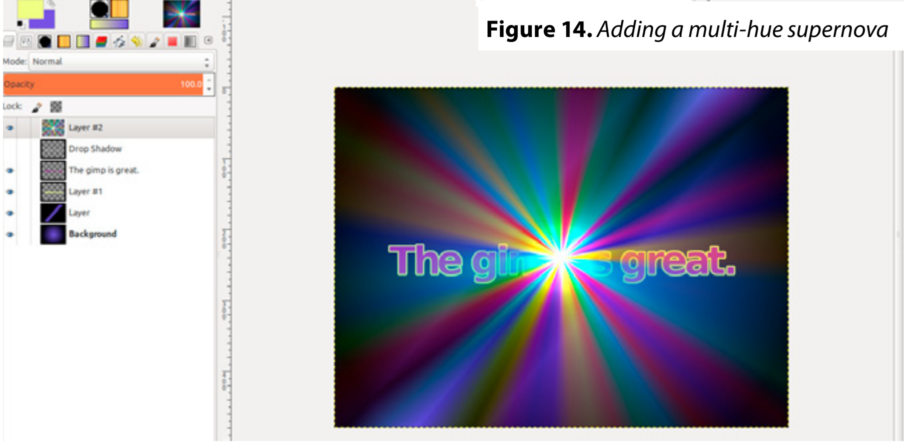
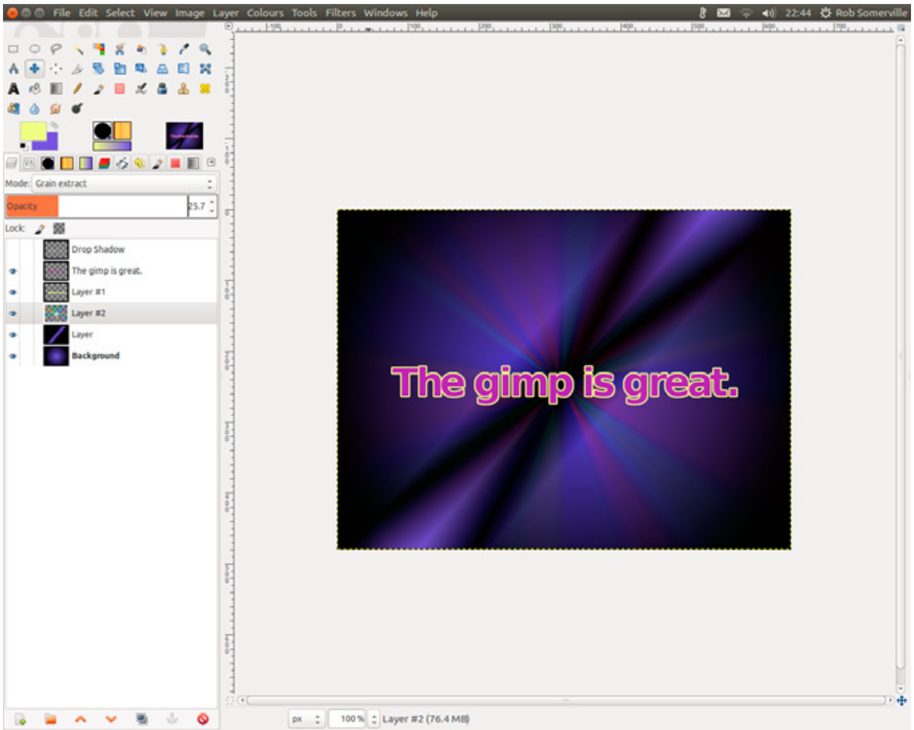


Figure 15. *Layer on top*

Step 14

Drag the layer behind Layer #1 and select Grain extract mode and 25% opacity Adjust so that the centre of the nova is in the middle of the "p" [Figure 16].


Mode: Grain extract

Opacity 25.7

Figure 16. *Layer behind text in grain extract mode and decreased opacity*

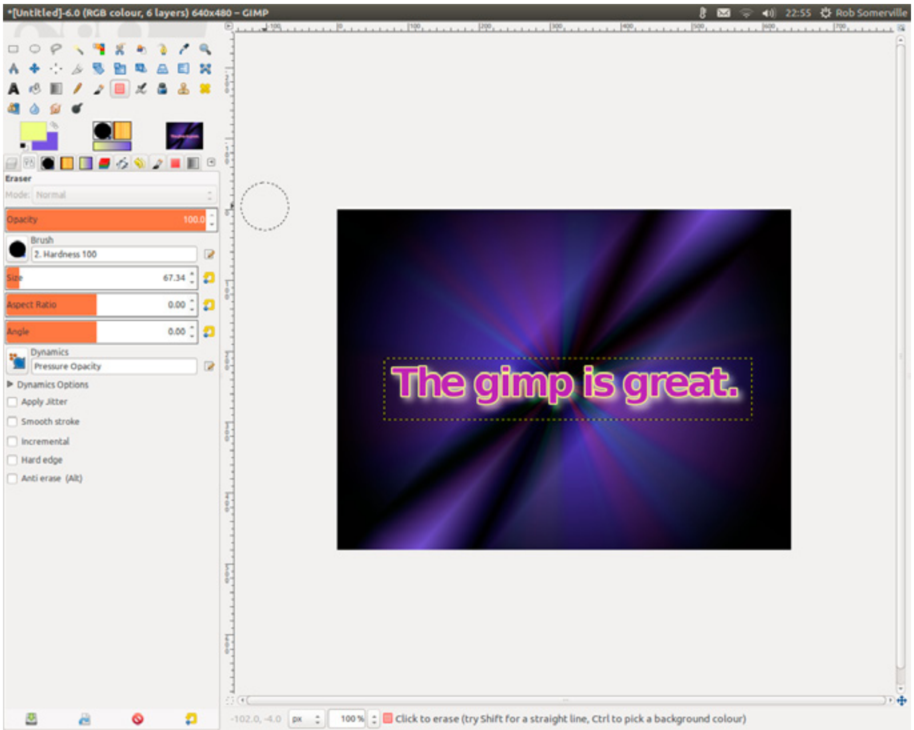
Step 15

Re-enable the shadow layer and drag below Layer #2. Adjust the opacity until the opacity gives the desired effect [Figure 17].

Step 16

Save the image as gimp.xcf and export to PNG or JPG to use in a website etc.

Once you have saved your XCF file, experiment with the layers, opacity and layer mode. Try different gradients blended in different modes.



*[Untitled]-6.0 (RGB colour, 6 layers) 640x480 – GIMP

Eraser

Mode: Normal

Opacity 100.0

Brush: 2. Hardness 100

Size 67.34

Aspect Ratio 0.00

Angle 0.00

Dynamics: Pressure Opacity

▶ Dynamics Options

□ Apply Jitter

□ Smooth stroke

□ Incremental

□ Hard edge

□ Anti erase (Alt)

-102.0, -4.0 px 100 % Click to erase (try Shift for a straight line, Ctrl to pick a background colour)

Figure 17. *The final image*

ROB SOMERVILLE

Rob Somerville has been passionate about technology since his early teens. A keen advocate of open systems since the mid-eighties, he has worked in many corporate sectors including finance, automotive, airlines, government and media in a variety of roles from technical support, system administrator, developer, systems integrator and IT manager. He has moved on from CP/M and nixie tubes but keeps a soldering iron handy just in case.

Resources

The Gimp website – *http://www.gimp.org*
Search Creative commons – *http://search.creativecommons.org*
Deviant art – *http://www.deviantart.com*
Stock.xchng – *http://www.sxc.hu*

The gimp is great.

Great Specials

On FreeBSD® & PC-BSD® Merchandise

Give us a call & ask about our
SOFTWARE BUNDLES
1.925.240.6652

$39.95
FreeBSD 9.1 Jewel Case CD Set
or FreeBSD 9.1 DVD

$29.95
PC-BSD 9.1 DVD

Save a BUNDLE!

$49.95
The PC-BSD 9.0 Users Handbook
PC-BSD 9.1 DVD

$99.95
The FreeBSD CD or DVD Bundle

Inside each CD/DVD Bundle, you'll find:
FreeBSD Handbook, 3rd Edition
Users Guide FreeBSD Handbook, 3rd Edition, Admin Guide
FreeBSD 9.1 CD or DVD set
FreeBSD Toolkit DVD

Stylish Dress Attire
Look Your Professional Best

Comfy Apparel
Stay Warm in Zip Ups & Pullovers

T-Shirts
Lots of Styles to Choose From

FreeBSD 9.1 Jewel Case CD/DVD $39.95

CD Set Contains:

Disc 1	Installation Boot LiveCD (i386)
Disc 2	Essential Packages Xorg (i386)
Disc 3	Essential Packages, GNOME2 (i386)
Disc 4	Essential Packages (i386)

FreeBSD 9.0 CD	$39.95
FreeBSD 9.0 DVD	$39.95

FreeBSD Subscriptions

Save time and $$$ by subscribing to regular updates of FreeBSD

FreeBSD Subscription, start with CD 9.1	$29.95
FreeBSD Subscription, start with DVD 9.1	$29.95
FreeBSD Subscription, start with CD 9.0	$29.95
FreeBSD Subscription, start with DVD 9.0	$29.95

PC-BSD 9.1 DVD (Isotope Edition)

PC-BSD 9.1 DVD	$29.95
PC-BSD Subscription	$19.95

The FreeBSD Handbook

The FreeBSD Handbook, Volume 1 (User Guide)	$39.95
The FreeBSD Handbook, Volume 2 (Admin Guide)	$39.95

The FreeBSD Handbook Specials

The FreeBSD Handbook, Volume 2 (Both Volumes)	$59.95
The FreeBSD Handbook, Both Volumes & FreeBSD 9.1	$79.95

PC-BSD 9.0 Users Handbook	$24.95
BSD Magazine	$11.99
The FreeBSD Toolkit DVD	$39.95
FreeBSD Mousepad	$10.00
FreeBSD & PCBSD Caps	$20.00
BSD Daemon Horns	$2.00

Bundle Specials!
Save $$$

Just Plain Fun
Mousepads & Novelty Horns

BSD Magazine
Available Monthly

FreeBSD Mall

For even MORE items
visit our website today!
www.FreeBSDMall.com

Set up a VOIP Server

for SIP Calls and protect it from bruteforce attacks in Ubuntu 12.04 LTS

In this tutorial I will show you how to set up a VOIP Server using Asterisk 1.8 and install FreePBX, a frontend interface for Asterisk, so that you can easily manage the Asterisk Server from a web interface and make it work without editing configuration files, writing dialplans and many other configurations.

What you will learn…

- installing Ubuntu 12.04 LTS, vi or pico text editor

What you should know…

- setting up a VOIP server and making SIP calls

VoIP is the initials for Voice Over Internet Protocol. It involves the transmission of voice signals over Internet lines and data networks. VoIP allows users to place phone calls from just about anywhere using broadband Internet.

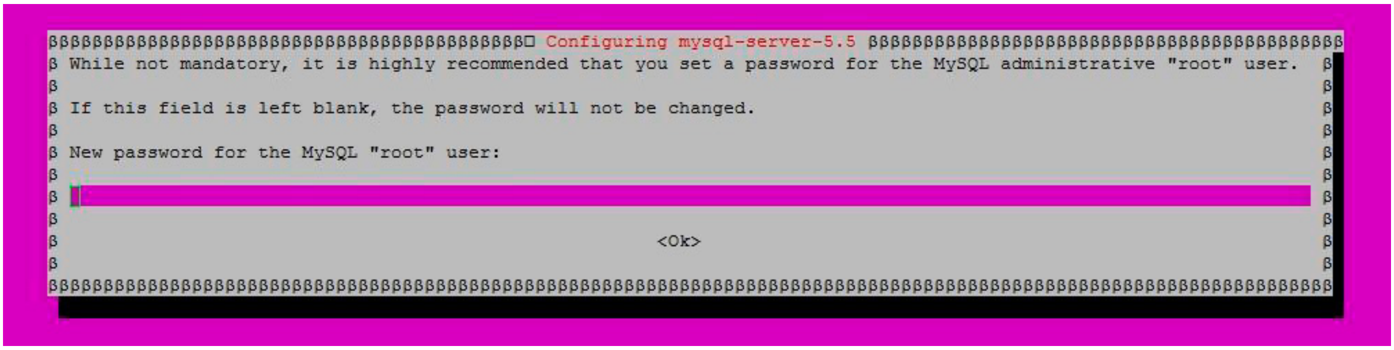
Asterisk is an open source framework for building communications applications. Asterisk turns an ordinary computer into a communications server. Asterisk powers IP PBX systems, VoIP gateways, conference servers and more. It is used by small businesses, large businesses, call centers, carriers and governments worldwide. Asterisk is free and sponsored by Digium. Now let's start our installation. Note that all shell commands that need to be executed on your machine start with "#".

Installing Asterisk 1.8.17

```
#aptitude update
#aptitude install -y mysql-server
```

Setup your root password for MySQL database

```
# aptitude update
#aptitude install -y build-essential linux-headers-`uname
   -r` linux-source bison flex apache2 php5 php5-curl php5-
   cli php5-mysql php-pear php-db php5-gd php5-mcrypt curl
   sox libncurses5-dev libssl-dev libmysqlclient15-dev
   mpg123 libxml2-dev ncurses-dev
```



```
ßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßß□ Configuring mysql-server-5.5 ßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßß
ß While not mandatory, it is highly recommended that you set a password for the MySQL administrative "root" user.  ß
ß                                                                                                                  ß
ß If this field is left blank, the password will not be changed.                                                   ß
ß                                                                                                                  ß
ß New password for the MySQL "root" user:                                                                          ß
ß                                                                                                                  ß
ß                                                                                                                  ß
ß                                                                                                                  ß
ß                                                    <Ok>                                                          ß
ß                                                                                                                  ß
ßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßßß
```

Figure 1. *Prompt to enter your MySQL root password*

```
#adduser asterisk --disabled-password --no-create-home
   --gecos “asterisk PBX user”
#adduser www-data asterisk

#cp /etc/apache2/apache2.conf /etc/apache2/apache2.conf_
   orig
#sed -i ‘s/^\(User\|Group\).*/\1 asterisk/’ /etc/apache2/
   apache2.conf
#/etc/init.d/apache2 restart
#cd /usr/src/
#tar xvjf linux-source-`echo $(uname -r) | sed -e “s/\-\
   (.*\)//”`.tar.bz2
#ln -s /usr/src/linux-source-`echo $(uname -r) | sed -e
   “s/\-\(.*\)//”` /usr/src/linux
#cd /usr/src/linux/
#make oldconfig
#make prepare
#make prepare scripts
#cd /usr/src/
```

Installing DAHDI

```
#wget http://downloads.digium.com/pub/telephony/dahdi-
   linux-complete/dahdi-linux-complete- 2.6.1+2.6.1.tar.gz
#tar xzvf dahdi-linux-complete-2.6.1+2.6.1.tar.gz
#rm -rf dahdi-linux-complete-2.6.1+2.6.1.tar.gz
#cd dahdi-linux-complete-2.6.1+2.6.1
#make all
#make install
#make config
#cd /usr/src/
```

Installing ASTERISK

```
#wget http://downloads.digium.com/pub/asterisk/releases/
   asterisk-1.8.17.0-rc1.tar.gz
#tar xzvf asterisk-1.8.17.0-rc1.tar.gz
#rm -rf asterisk-1.8.17.0-rc1.tar.gz
#cd asterisk-1.8.17.0-rc1
#./configure
#make menuconfig

select app_mysql, app_saycountpl, cdr_mysql, format_mp3,
   res_config_mysql
go to Extras Sound Packages
Select EXTRAS-SOUNDS-EN-GSM
Save & Exit

#make
#make install
#make samples
#cd /usr/src/

#ln -s /lib/modules/`echo $(uname -r) | sed -e “s/\-\
   (.*\)//”`/ /lib/modules/$(uname -r)/asterisk
#depmod
#echo dahdi_dummy >> /etc/modules
```

Installing Asterisk Sounds

```
#mkdir /var/lib/asterisk/sounds/
#cd /var/lib/asterisk/sounds/
#wget http://downloads.asterisk.org/pub/telephony/sounds/
   releases/asterisk-core-sounds-en-wav-1.4.22.tar.gz
#wget http://downloads.asterisk.org/pub/telephony/sounds/
   releases/asterisk-core-sounds-en-sln16-1.4.22.tar.gz
#wget http://downloads.asterisk.org/pub/telephony/sounds/
   releases/asterisk-core-sounds-en-gsm-1.4.22.tar.gz
#wget http://downloads.asterisk.org/pub/telephony/sounds/
   releases/asterisk-core-sounds-en-g729-1.4.22.tar.gz

#wget http://downloads.asterisk.org/pub/telephony/sounds/
   releases/asterisk-extra-sounds-en-sln16-1.4.11.tar.gz
#wget http://downloads.asterisk.org/pub/telephony/sounds/
   releases/asterisk-extra-sounds-en-wav-1.4.11.tar.gz
#wget http://downloads.asterisk.org/pub/telephony/sounds/
   releases/asterisk-extra-sounds-en-gsm-1.4.11.tar.gz
#wget http://downloads.asterisk.org/pub/telephony/sounds/
   releases/asterisk-extra-sounds-en-g729-1.4.11.tar.gz

#tar xzvf asterisk-core-sounds-en-wav-1.4.22.tar.gz
#tar xzvf asterisk-core-sounds-en-sln16-1.4.22.tar.gz
#tar xzvf asterisk-core-sounds-en-gsm-1.4.22.tar.gz
#tar xzvf asterisk-core-sounds-en-g729-1.4.22.tar.gz

#tar xzvf asterisk-extra-sounds-en-sln16-1.4.11.tar.gz
#tar xzvf asterisk-extra-sounds-en-wav-1.4.11.tar.gz
#tar xzvf asterisk-extra-sounds-en-gsm-1.4.11.tar.gz
#tar xzvf asterisk-extra-sounds-en-g729-1.4.11.tar.gz

#rm -rf asterisk-core-sounds-en-wav-1.4.22.tar.gz
#rm -rf asterisk-core-sounds-en-sln16-1.4.22.tar.gz
#rm -rf asterisk-core-sounds-en-gsm-1.4.22.tar.gz
#rm -rf asterisk-core-sounds-en-g729-1.4.22.tar.gz
#rm -rf asterisk-extra-sounds-en-sln16-1.4.11.tar.gz
#rm -rf asterisk-extra-sounds-en-wav-1.4.11.tar.gz
#rm -rf asterisk-extra-sounds-en-gsm-1.4.11.tar.gz
#rm -rf asterisk-extra-sounds-en-g729-1.4.11.tar.gz
```

Fix up directory use and permissions for asterisk

```
#chown -R asterisk:asterisk /var/lib/asterisk/sounds/
#mkdir /var/run/asterisk
#chown asterisk:asterisk -Rv /var/run/asterisk
#chown asterisk:asterisk -Rv /etc/asterisk
#chown asterisk:asterisk -Rv /var/lib/asterisk
#chown asterisk:asterisk -Rv /dev/zap
#chown asterisk:asterisk -Rv /var/log/asterisk
#chown asterisk:asterisk -Rv /var/spool/asterisk
```

Moh fix

```
#ln -s /var/lib/asterisk/moh /var/lib/asterisk/mohmp3
#chown asterisk:asterisk /var/lib/asterisk/mohmp3
```

Create asterisk logrotate

```
#touch /etc/logrotate.d/asterisk
#vi /etc/logrotate.d/asterisk
```

Add the lines below:

```
 /var/log/asterisk/*log {
 missingok
 rotate 5
 weekly
 create 0640 asterisk asterisk
 postrotate
 /usr/sbin/asterisk -rx ‘logger reload’ > /dev/null 2> /
   dev/null
 endscript
 }
 /var/log/asterisk/full {
 missingok
 rotate 5
 daily
 create 0640 asterisk asterisk
 postrotate
 /usr/sbin/asterisk -rx ‘logger reload’ > /dev/null 2> /
   dev/null
 endscript
 }
/var/log/asterisk/cdr-csv/*csv {
 missingok
 rotate 5
 monthly
 create 0640 asterisk asterisk
 }
```

Install phpmyadmin to manage mysql

```
#cd /usr/src
#wget http://sourceforge.net/projects/phpmyadmin/files/
   phpMyAdmin/3.5.2.2/phpMyAdmin-3.5.2.2-all-languages.
   tar.gz
#tar -xzvf phpMyAdmin-3.5.2.2-all-languages.tar.gz
#rm -f phpMyAdmin-3.5.2.2-all-languages.tar.gz
#mv phpMyAdmin-3.5.2.2-all-languages /var/www/phpmyadmin
```

Installing FreePBX

```
#cd /usr/src/
#wget http://mirror.FreePBX.org/FreePBX-2.9.0.tar.gz
#tar -zxvf FreePBX-2.9.0.tar.gz
#rm -rf FreePBX-2.9.0.tar.gz

#configure FreePBX
#cd FreePBX-2.9.0
```

Setup databases for FreePBX use

```
#mysqladmin -u root -pENTER_YOUR_MYSQL_ROOT_PASSWORD_HERE
   create asterisk
#mysqladmin -u root -pENTER_YOUR_MYSQL_ROOT_PASSWORD_HERE
   create asteriskcdrdb
#mysql -u root -pENTER_YOUR_MYSQL_ROOT_PASSWORD_HERE
   asterisk < SQL/newinstall.sql
#mysql -u root -pENTER_YOUR_MYSQL_ROOT_PASSWORD_HERE
   asteriskcdrdb < SQL/cdr_mysql_table.sql
#mysql -u root -pENTER_YOUR_MYSQL_ROOT_PASSWORD_HERE
   <<-END_PRIVS
>GRANT ALL PRIVILEGES ON asterisk.* TO asteriskuser@
   localhost IDENTIFIED BY “ENTER_YOUR_ASTERISK_DB_
   PASSWORD_HERE”;
>GRANT ALL PRIVILEGES ON asteriskcdrdb.* TO asteriskuser@
   localhost IDENTIFIED BY “ENTER_YOUR_ASTERISK_DB_
   PASSWORD_HERE”;
>flush privileges;
>END_PRIVS
```

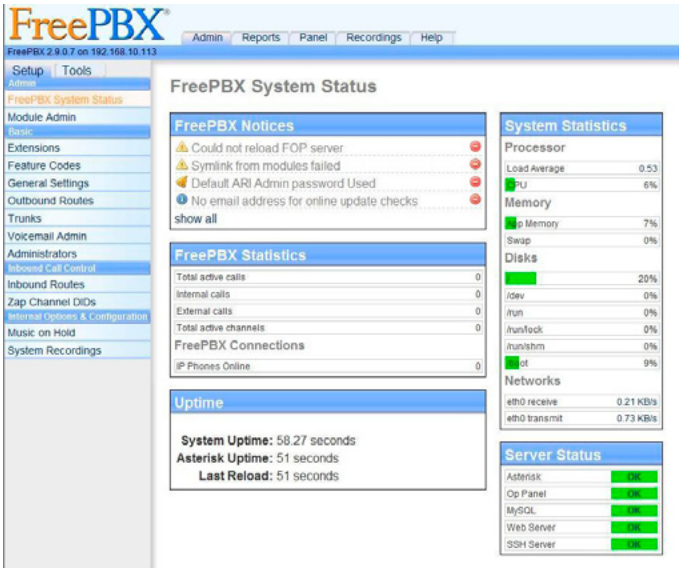
Reconfigure php for FreePBX

```
#cp -v /etc/php5/apache2/php.ini /etc/php5/apache2/php.
   ini-orig
#cp /etc/php5/apache2/php.ini /etc/php5/php.ini
#rm -rf /etc/php5/apache2/php.ini
#rm -rf /etc/php5/cli/php.ini
#ln -s /etc/php5/php.ini /etc/php5/apache2/php.ini
#ln -s /etc/php5/php.ini /etc/php5/cli/php.ini

#sed -i “s/\(upload_max_filesize *= *\)\(.*\)/\120M/” /etc/
```

```
    php5/php.ini
#sed -i “s/\(memory_limit *= *\)\(.*\)/\1100M/” /etc/php5/
    php.ini
```

Fix up directory use and permissions for asterisk

```
#mkdir /var/www/html/
#chown asterisk:asterisk -Rv /var/www/html

# configure amportal
#cp -v amportal.conf /etc/amportal.conf
#echo “AMPDBUSER=asteriskuser”>> /etc/amportal.conf
#echo “AMPDBPASS=ENTER_YOUR_ASTERISK_DB_PASSWORD_HERE” >>
    /etc/amportal.conf
#echo “AMPWEBADDRESS=ENTER_YOUR_IP_ADDRESS_HERE” >> /etc/
    amportal.conf
#echo “AMPMGRPASS=ENTER_YOUR_ASTERISK_MGR_PASSWORD_HERE”
    >> /etc/amportal.conf
#./start_asterisk start
#./install_amp
```



FreePBX System Status

FreePBX Notices
- Could not reload FOP server
- Symlink from modules failed
- Default ARI Admin password Used
- No email address for online update checks

show all

FreePBX Statistics

Total active calls	0
Internal calls	0
External calls	0
Total active channels	0

FreePBX Connections

IP Phones Online	0

Uptime

System Uptime: 58.27 seconds
Asterisk Uptime: 51 seconds
Last Reload: 51 seconds

System Statistics

Processor

Load Average	0.53
CPU	6%

Memory

App Memory	7%
Swap	0%

Disks

/	20%
/dev	0%
/run	0%
/run/lock	0%
/run/shm	0%
/boot	9%

Networks

eth0 receive	0.21 KB/s
eth0 transmit	0.73 KB/s

Server Status

Asterisk	OK
Op Panel	OK
MySQL	OK
Web Server	OK
SSH Server	OK

Figure 2. *FreePBX 2.9.0.7 running after installation*

Set ARI admin password

```
#sed -i “s/ari_password/YOUR_ARI_PASSWORD_HERE/” /var/www/
    html/recordings/includes/main.conf.php
```

Start amportal at boot

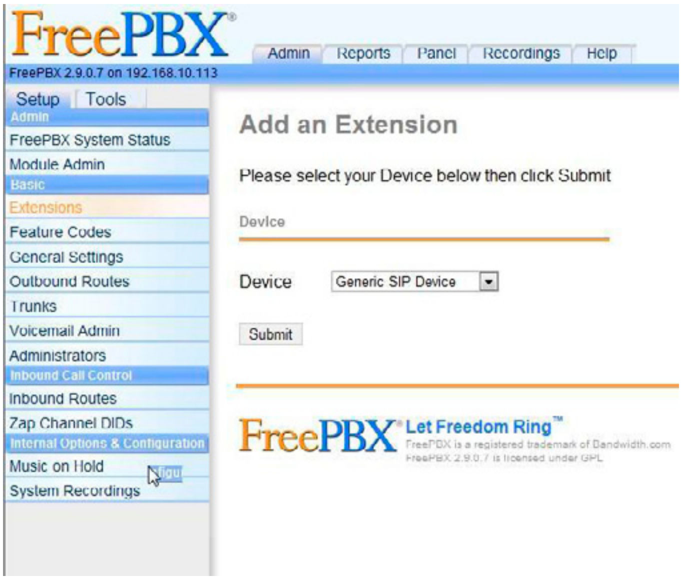
```
#echo “/usr/local/sbin/amportal start” > /etc/rc.local
#echo “exit 0” >> /etc/rc.local
```

Start FreePBX

```
#/usr/local/sbin/amportal start
```

To check if FreePBX is running, we go to our browser and enter the URL: *http://server_ip/html/admin* (Figure 2). The default username is admin and password admin to login to the admin menu.

Now let’s create SIP accounts so we can call from SIP to SIP. We click on the FreePBX panel. The link extension will direct you to “Add an Extension Page” (Figure 4).



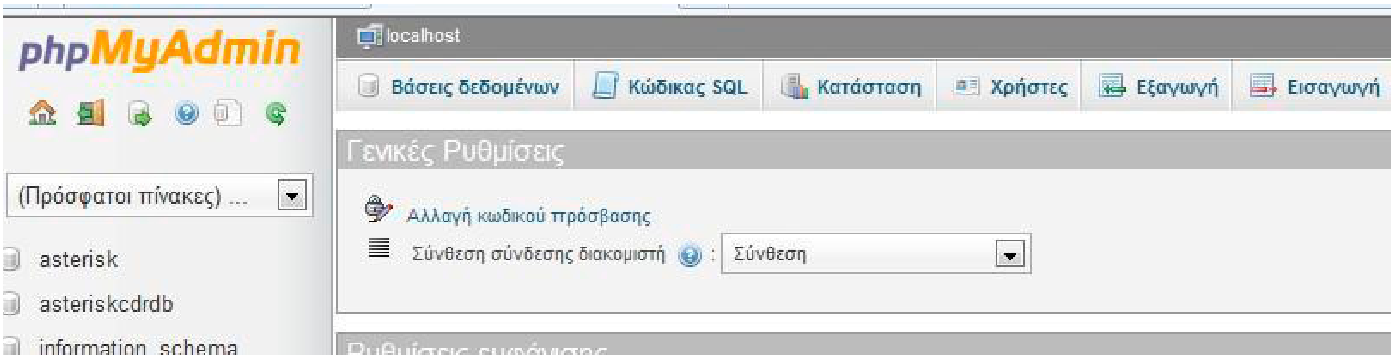
Add an Extension

Please select your Device below then click Submit

Device

Device: Generic SIP Device

Figure 4. *Add an Extension FreePBX page*



asterisk
asteriskcdrdb
information_schema

Γενικές Ρυθμίσεις

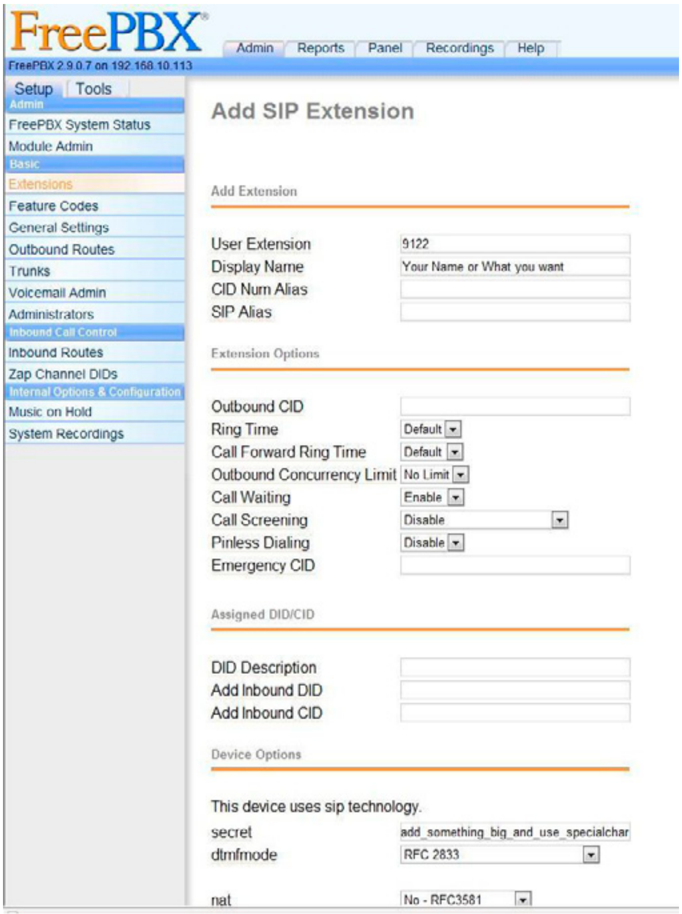
Σύνθεση σύνδεσης διακομιστή: Σύνθεση

Ρυθμίσεις εμφάνισης

Figure 3. *Asterisk and FreePBX Mysql tables*

We click submit on this page. In the new page that opens, we fill User Extension with the number that you want to have for the User, the Display Name that will show when this user calls you, and the secret password it will use to register to the Asterisk server. It is best to use a long password with both lower and upper case letters and special characters like "#$%*^". (Figure 5)

After we create our SIP accounts, we need phones in order to make SIP calls. There are softphones for smartphones and computers and also hardware VOIP Telephones. One very good SIP softphone for Windows is XLite (*http://www.counterpath.com/x-lite.html*). For Linux and many other systems, it is Linphone (*http://www.linphone.org*). There are many other softphones. A search on the internet using the keywords "free voip softphones" will reveal many results. You can figure out how to configure them and make calls by browsing the website of the softphone that you choose. A good idea is to buy a hardware VOIP phone so that you can call directly without the need of a computer.



Add SIP Extension

Add Extension

User Extension	9122
Display Name	Your Name or What you want
CID Num Alias	
SIP Alias	

Extension Options

Outbound CID	
Ring Time	Default
Call Forward Ring Time	Default
Outbound Concurrency Limit	No Limit
Call Waiting	Enable
Call Screening	Disable
Pinless Dialing	Disable
Emergency CID	

Assigned DID/CID

DID Description	
Add Inbound DID	
Add Inbound CID	

Device Options

This device uses sip technology.

secret	add_something_big_and_use_specialchar
dtmfmode	RFC 2833
nat	No - RFC3581

Figure 5. *Create a user extension for SIP calls*

Figure 6. *X-Lite for windows softphone*

SECURING ASTERISK FROM SIP BRUTEFORCE ATTACKS

To secure Asterisk from bruteforce attacks that try to find an extension number and password, we will use Fail2Ban. Fail2Ban works by scanning log files and then taking action based on the entries in those logs.

We are implementing Fail2Ban with a configuration to prevent SIP brute force attacks against our Asterisk PBXs.

Installing Fail2Ban

```
#aptitude install fail2ban
#cd /etc/fail2ban/
```

Configuring Fail2Ban

```
#vi jail.conf
```

add after

```
[apache-overflows]

enabled = true
port    = 2985,29443
filter  = apache-overflows
logpath = /var/log/apache*/*error.log
maxretry = 2
```

the text below

```
[asterisk-iptables]

enabled  = true
filter   = asterisk
action   = iptables-allports[name=ASTERISK, protocol=all]
           sendmail-whois[name=ASTERISK, dest=root@
   localhost, sender=fail2ban@localhost]
logpath  = /var/log/asterisk/messages
```

```
maxretry = 3
bantime = 96400
```

then

```
#cd /etc/fail2ban/filter.d/
create a file asterisk.conf
#touch /etc/fail2ban/filter.d/asterisk.conf
```

And add the lines below in this files save and close it

```
#Fail2Ban configuration file
#
#
# $Revision: 250 $
#

[INCLUDES]

# Read common prefixes. If any customizations available --
   read them from
# common.local
#before = common.conf


[Definition]

#_daemon = asterisk

# Option:  failregex
# Notes.:  regex to match the password failures messages
   in the logfile. The
#          host must be matched by a group named “host”.
   The tag “<HOST>” can
#          be used for standard IP/hostname matching and
   is only an alias for
#          (?:::f{4,6}:)?(?P<host>\S+)
# Values:  TEXT
#

failregex = Registration from ‘.*’ failed for
   ‘<HOST>(:[0-9]{1,5})?’ - Wrong password
           Registration from ‘.*’ failed for
   ‘<HOST>(:[0-9]{1,5})?’ - No matching peer found
           Registration from ‘.*’ failed for
   ‘<HOST>(:[0-9]{1,5})?’ - Device does not match ACL
           Registration from ‘.*’ failed for
   ‘<HOST>(:[0-9]{1,5})?’ - Username/auth name mismatch
           Registration from ‘.*’ failed for
   ‘<HOST>(:[0-9]{1,5})?’ - Peer is not supposed to
   register
           NOTICE.* <HOST> failed to authenticate as
   ‘.*’$
           NOTICE.* .*: No registration for peer ‘.*’
   (from <HOST>)
           NOTICE.* .*: Host <HOST> failed MD5
   authentication for ‘.*’ (.*)
           VERBOSE.* logger.c: -- .*IP/<HOST>-.* Playing
   ‘ss-noservice’ (language ‘.*’)

# Option:  ignoreregex
# Notes.:  regex to ignore. If this regex matches, the
   line is ignored.
# Values:  TEXT
#
ignoreregex =
then restart fail2ban

#/etc/init.d/fail2ban restart
```

Also keep in mind

- Install a basic firewall to protect your ports and leave specific access to your server per IP.
- Access your FreePBX remotely using https. For this, you need to install certificates on Apache. In this tutorial, the Apache is using plain http.
- Protect your FreePBX folder using htaccess and if is possible from static IP.
- Don’t use the default port 5060 for Asterisk.
- You can also extend your Asterisk to make calls to landlines and mobiles using trunks and outbound routes.

STAVROS N. SHIAELES (PH.D)

Is a member of the IEEE and the IEEE Computer Society. He received his MEng diploma in Electrical and Computer Engineering (DUTH) in 2007 and Ph.D in 2013. He has worked in various operating systems in IT and as a consultant for many companies. Currently he is a researcher in the area of Computer Security.

Network Analysis On a Storage Area Network Using Wireshark

Wireshark, originally known as Ethereal, is probably the most famous open source packet sniffer and network analysis tool available.

What you will learn…

- How to use Wireshark in a SAN environment

What you should know…

- Basic security skills

This application supports about 1300 protocols through a vast number of filters. Functionalities such as traffic, protocol analysis, and packet dissector make it an extremely versatile tool for security experts, network engineers, and system administrators.

Wireshark can be used during a proactive analysis to identify potential network bottlenecks, to monitor "live" what is happening to data flow, and to decode packets in transit, displaying information in readable format. The tool can be installed on any computer connected to the network and equipped with a NIC card. Using specific API or libraries, such as WinPcap under Windows or libpcap for Unix, it enables data capture and allows analysis of packets travelling over the carrier. Commonly, Wireshark is used on Ethernet technology or Wireless networks, but it's also possible to use it for a SAN (*Storage Area Network*) to analyze FCP (*Fiber Channel Protocol*) over Optical Fiber Cables.

The Storage Area Network Architecture

SAN (*Storage Area Network*) is generally defined as a dedicated storage network using Fibre Channel technology to provide disk volumes on the target host.

The SAN environment can be designed to have a disk array directly attached to a host or through a SAN Switch (a SAN Network Director similar to the Ethernet Switch) in order to connect multiple hosts to a single array and enable Business Continuity and Disaster Recovery capabilities.

Disks' capacities are presented as logical volumes called LUNs (Logic Unit Numbers). The provisioning is performed by connecting the Array, Switch and HBA (Host Bus Adapter, a fiber card adapter installed on the Host system) using two different operations called LUN Masking and Zoning (Figure 1).

With Zoning, we connect the ports of the devices, also called initiators, to be logically linked. While performing the LUN Masking, we present the LUN (disk capacity) to the target host.

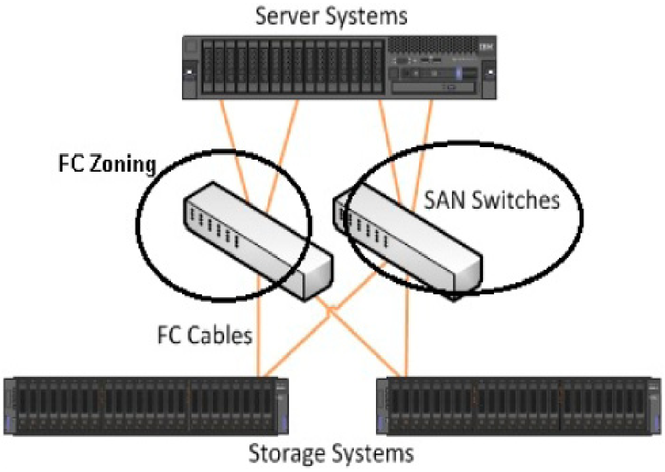


Figure 1. *Fiber Channel Zoning*

The SAN directors are accessible by Storage and Network Administrators via the Terminal Access Controller Access-Control System (TACACS) or the Remote Authentication Dial In User Service (RADIUS).

The main difference between NAS and SAN volume provisioning systems is the protocol used to provide storage capacity. NAS uses NFS or CIFS protocols, while SAN uses the FCP (Fiber Channel Protocol).

Fiber Channel Protocol

The FCP (Fibre Channel Protocol) is a transport protocol similar to TCP/IP, approved as ANSI standard around 1994. FCP mainly transports SCSI commands using the Optical Cable as a carrier (Figure 2).

This protocol was invented to enable higher performances and distance insensitivity, to facilitate the system boot from external devices and support enterprise storage flexibility and scalability.

Fiber Channel Traffic Analysis

Network analysis on a fiber channel is not the same as on the Ethernet. There's no equivalent promiscuous mode for nodes, so you can't listen to traffic moving through the network. To achieve traffic analysis, you have to tap into the network between the source and destination ports you wish to analyze. A dedicated hardware is necessary to "read" the packets and specific software to analyze the frames.

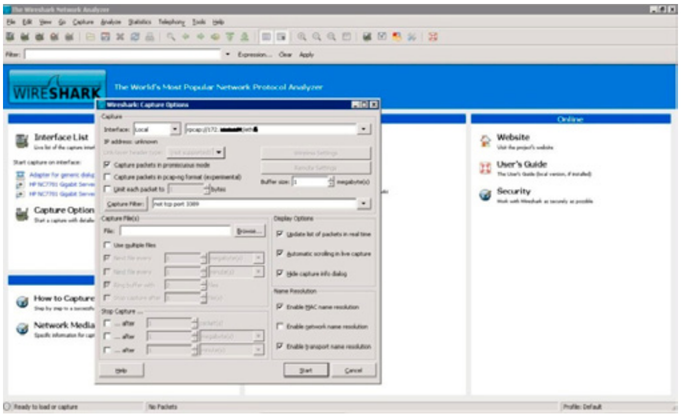
Some examples of external frame analyzers are: Xgig Protocol Analyzer Family from JDSU or LeCroy FC Protocol Analyzers.

FC frame analyzers are often accompanied by a dedicated TAP (*Traffic Access Point*) network hardware. This device is physically inserted into the network and when turned on, it copies all frames headed for a specific port to a specific TAP port. Using TAP hardware means that the frame analyzer can be plugged into the TAPped port and then removed without causing an interruption in the FC network flow. Of course, in order to initially install the TAP hardware, you have to interrupt the network flow.

Preferably, these devices should be permanently connected, because each time you insert and remove the analyzer, you interrupt the FC network flow. This may end up in serious repercussions for the system, such as Data Loss and Kernel Panic.

In some cases, this has been made easier by Vendors such as Cisco and Brocade, providing a *Switched Port Analyzer* (SPAN) feature, which copies most traffic going to a specific port to another switch port "called mirror port."

Figure 2. *Fiber Cable*



The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter: Expression... Clear Apply
WIRESHARK
The World's Most Popular Network Protocol Analyzer
Interface List
Start capture on interface:
Capture Options
How to Capture
Network Media
Online
Website
User's Guide
Security
Wireshark: Capture Options

Capture

Interface: Local rpcap://172.[redacted]/eth0

IP address: unknown

☑ Capture packets in promiscuous mode

☐ Capture packets in pcap-ng format (experimental)

☐ Limit each packet to bytes

Buffer size: 1 megabyte(s)

Capture Filter: not tcp port 3389

Capture File(s)

File: Browse...

☐ Use multiple files

Display Options

☑ Update list of packets in real time

☑ Automatic scrolling in live capture

☑ Hide capture info dialog

Name Resolution

☑ Enable MAC name resolution

☐ Enable network name resolution

☑ Enable transport name resolution

Stop Capture ...

☐ ... after

☐ ... after

☐ ... after

Help Start Cancel

Ready to load or capture No Packets Profile: Default

Figure 4. *Setting up Wireshark*

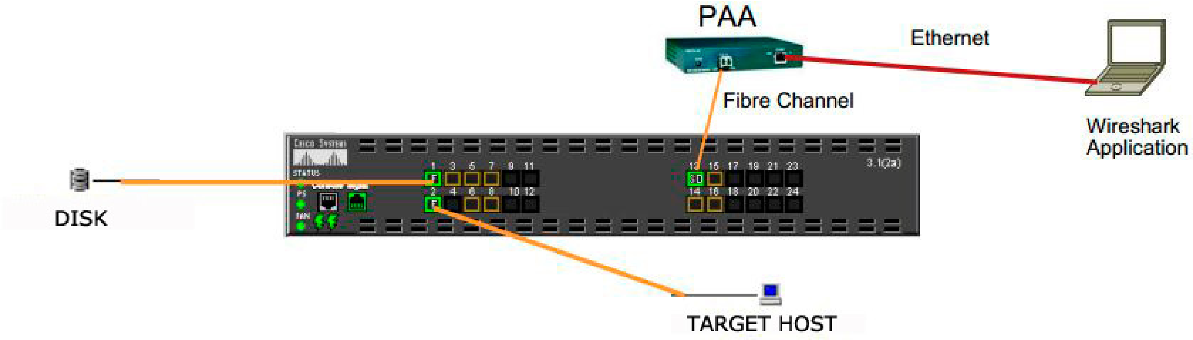


Figure 3. *Typical SPAN to PAA Configuration*

In that case, the frame analyzer or PAA (*Protocol Analyzer Adapter*) can be plugged into the SPAN switch port and the traffic flow can be analyzed. (Figure 3)

Cisco and Brocade provide native command line tools to allow local fiber channel control traffic passing through the local supervisors to be copied into a text file that is stored in a chosen location on the switch or redirected to an IP Address.

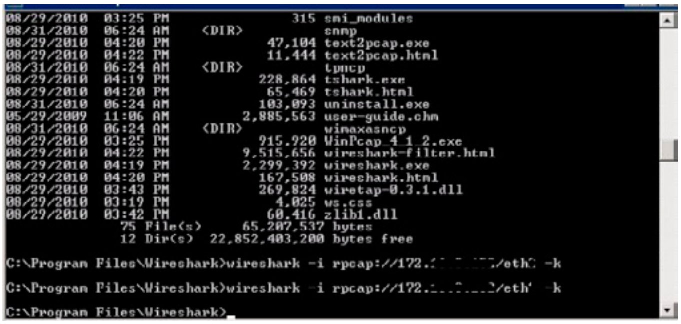
The default behavior is to store the output in a volatile storage area. This can later be copied to a remote server for analysis with Wireshark.

It is also possible to specify a remote IP address to send the data to, and Wireshark can be used to analyze the data in real time, as it's collected.

Cisco MDS Switches with the SanOS operating system provide an FC Analyzer command line called: *fcanalyzer* (portlogshow is the command line on brocade).

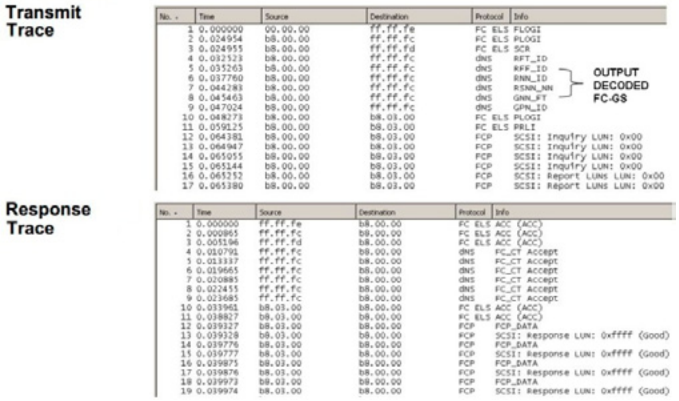
In order to configure the system to perform traffic analysis, we must configure the Switch in passive remote mode using the command line as follows:

```
MDS3(config)# fcanalyzer remote 172.xxx.xxx.xxx
MDS3(config)# exit
MDS3# show fcanalyzer
PassiveClient = 172.xxx.xxx.xxx
MDS2#
```



```
08/29/2010  03:25 PM               315 smi_modules
08/31/2010  06:24 AM    <DIR>          snmp
08/29/2010  04:20 PM            47,104 text2pcap.exe
08/29/2010  04:22 PM            11,444 text2pcap.html
08/31/2010  06:24 AM    <DIR>          tpncp
08/29/2010  04:19 PM           228,864 tshark.exe
08/29/2010  04:20 PM            65,469 tshark.html
08/31/2010  06:24 AM           103,093 uninstall.exe
05/29/2009  11:06 AM         2,885,563 user-guide.chm
08/31/2010  06:24 AM    <DIR>          wimaxasncp
08/29/2010  03:25 PM           915,920 WinPcap_4_1_2.exe
08/29/2010  04:22 PM         9,515,656 wireshark-filter.html
08/29/2010  04:19 PM         2,299,392 wireshark.exe
08/29/2010  04:20 PM           167,508 wireshark.html
08/29/2010  03:43 PM           269,824 wiretap-0.3.1.dll
08/29/2010  03:19 PM             4,025 ws.css
08/29/2010  03:42 PM            60,416 zlib1.dll
              75 File(s)     65,207,537 bytes
              12 Dir(s)  22,852,403,200 bytes free

C:\Program Files\Wireshark>wireshark -i rpcap://172.[redacted]/eth[redacted] -k

C:\Program Files\Wireshark>wireshark -i rpcap://172.[redacted]/eth[redacted] -k

C:\Program Files\Wireshark>_
```

Figure 5. *Remote Connection via Command Line Interface*



No.	Time	Source	Destination	Protocol	Info
1	0.000000	00.00.00	ff.ff.fe	FC ELS	FLOGI
2	0.024954	b8.00.00	ff.ff.fc	FC ELS	PLOGI
3	0.024955	b8.00.00	ff.ff.fd	FC ELS	SCR
4	0.032523	b8.00.00	ff.ff.fc	dNS	RFT_ID
5	0.035263	b8.00.00	ff.ff.fc	dNS	RFF_ID
6	0.037760	b8.00.00	ff.ff.fc	dNS	RNN_ID
7	0.044283	b8.00.00	ff.ff.fc	dNS	RSNN_NN
8	0.045463	b8.00.00	ff.ff.fc	dNS	GNN_FT
9	0.047024	b8.00.00	ff.ff.fc	dNS	GPN_ID
10	0.048273	b8.00.00	b8.03.00	FC ELS	PLOGI
11	0.059125	b8.00.00	b8.03.00	FC ELS	PRLI
12	0.064381	b8.00.00	b8.03.00	FCP	SCSI: Inquiry LUN: 0x00
13	0.064947	b8.00.00	b8.03.00	FCP	SCSI: Inquiry LUN: 0x00
14	0.065055	b8.00.00	b8.03.00	FCP	SCSI: Inquiry LUN: 0x00
15	0.065144	b8.00.00	b8.03.00	FCP	SCSI: Inquiry LUN: 0x00
16	0.065252	b8.00.00	b8.03.00	FCP	SCSI: Report LUNS LUN: 0x00
17	0.065380	b8.00.00	b8.03.00	FCP	SCSI: Report LUNS LUN: 0x00

No.	Time	Source	Destination	Protocol	Info
1	0.000000	ff.ff.fe	b8.00.00	FC ELS	ACC (ACC)
2	0.000865	ff.ff.fc	b8.00.00	FC ELS	ACC (ACC)
3	0.005196	ff.ff.fd	b8.00.00	FC ELS	ACC (ACC)
4	0.010791	ff.ff.fc	b8.00.00	dNS	FC_CT Accept
5	0.013337	ff.ff.fc	b8.00.00	dNS	FC_CT Accept
6	0.019665	ff.ff.fc	b8.00.00	dNS	FC_CT Accept
7	0.020885	ff.ff.fc	b8.00.00	dNS	FC_CT Accept
8	0.022455	ff.ff.fc	b8.00.00	dNS	FC_CT Accept
9	0.023685	ff.ff.fc	b8.00.00	dNS	FC_CT Accept
10	0.033961	b8.03.00	b8.00.00	FC ELS	ACC (ACC)
11	0.038827	b8.03.00	b8.00.00	FC ELS	ACC (ACC)
12	0.039327	b8.03.00	b8.00.00	FCP	FCP_DATA
13	0.039328	b8.03.00	b8.00.00	FCP	SCSI: Response LUN: 0xffff (Good)
14	0.039776	b8.03.00	b8.00.00	FCP	FCP_DATA
15	0.039777	b8.03.00	b8.00.00	FCP	SCSI: Response LUN: 0xffff (Good)
16	0.039875	b8.03.00	b8.00.00	FCP	FCP_DATA
17	0.039876	b8.03.00	b8.00.00	FCP	SCSI: Response LUN: 0xffff (Good)
18	0.039973	b8.03.00	b8.00.00	FCP	FCP_DATA
19	0.039974	b8.03.00	b8.00.00	FCP	SCSI: Response LUN: 0xffff (Good)

Figure 6. *Host Login Trace*

Next, we instruct Wireshark to connect to it remotely using the graphical interface (Figure 4). Or, we may try to connect it using the Wireshark CLI (Figure 5). Now, we are ready to start a new capture session and verify which type of raw data we can get out of the FC analyzer.

Wireshark can capture a huge amount of information, when installed between the disk array and the host machine. It could potentially intercept all the SCSI commands passing through these two devices. At the same time, it is possible to inspect what is happening at the switch level and use the data for troubleshooting and debugging purposes.

During a live capture session, we can monitor the Fabric behavior, the Zone-sets operations, or we can display which initiators and nodes are currently active and enabled.

It is possible to verify volumes presented to the hosts and potentially reverse engineer the entire SAN configuration.

If we can manage to identify all the Zoning and Masking setup and if the Switch is using features such as VSAN (Virtual SAN similar to VLAN in Ethernet Networks) or IVR (Inter-VSAN Routing), we can trace all the members' devices existing in all of the SAN area including all the SCSI command dialogs.

With the help of customized filters, it is possible to use Wireshark for troubleshooting purposes and display (for example, merge conflicts, Fabric Login status, Zoning failure, and so on). A good example is visible in Figure 6. We can see a live capture session with Wireshark tracing a Host Login event. It is possible to trace the entire "dialog" between the Host and the Remote Array through the Switches. There are two active windows in Wireshark:

- Transmit Trace
- Response Trace

The first one is tracing the FCP/SCSI transmission dialog and the second traces the responses.

In the first window, we can see LUNs (remote disks) are in "inquiry status" (seeking to log on to target host) and the FC initiator is attempting to initiate the FLOGI (a link service command that sets up a session between two participants' devices).

We can verify the positive response in the second window. The Login request is accepted and we can see the positive response. The trace window is now displaying that LUNs are reported in good status, hence available to be mounted on the target Host.

Conclusions

This article provides a quick overview of using Wireshark in a SAN environment. Although, network analyzers are powerful software and can be used to troubleshoot complicated issues, at the same time, they can be extremely dangerous when misused or activated through unauthorized access.

Sniffers are difficult to detect and can be applied almost anywhere within the network under analysis, which makes it one of the hackers' favorite tools.

We need to bear in mind that NO Firewalls or IDS are present in a SAN environment; thus it is not possible to filter traffic or identify intruders easily.

The Login of a "new" device in the fabric is never reported as a malicious activity and poorly monitored. Moreover a volume can be mounted and shared over multiple hosts and, in most cases, there is no event alert that traces the activity.

It's true that SAN protocol presents all the data at block level, but it is still possible to capture and dump, in a separate storage area, a large quantity of traffic to attempt file reconstructions later.

Using Wireshark to perform SAN network cartography may be a good starting point to perform further attacks. One may be able to use the information gathered to reconfigure Zoning and Masking, mount the target volume on a different Host, and gain access to stored data.

FCP is a protocol that does not provide encryption, thus all the data travelling is potentially exposed.

Remember to handle all the information gathered with Wireshark carefully in order to avoid data leakage. We should store all the captured files securely, possibly in encrypted volumes and never forget that sniffing is an illegal activity when performed without authorization.

Appendix 1

- *http://www.cisco.com/en/US/docs/switches/datacenter/mds9000/sw/4_1/configuration/guides/cli_4_1/tsf.html*
- *http://en.wikipedia.org/wiki/Fibre_Channel*
- *http://en.wikipedia.org/wiki/Fibre_Channel_Logins*
- *http://en.wikipedia.org/wiki/Fibre_Channel_zoning*
- *http://www.jdsu.com/en-us/Test-and-Measurement/Products/a-z-product-list/Pages/xgig-protocol-analyzer-family-overview.aspx*
- *http://teledynelecroy.com/protocolanalyzer/protocolstandard.aspx?standardid=5*
- *http://www.brocade.com/products/all/switches/index.page*
- *http://www.cisco.com/en/US/products/hw/ps4159/ps4358/products_configuration_example09186a008026eb55.shtml*

SEMBIANTE MASSIMILIANO

M.S.c. Computer Security Employed at UBS Bank as an IT Security and Risk Specialist. Collaborating as a Research Engineer at R.I.F.E.C. (Research Institute of Forensic and E-Crimes) focusing on: New Virus, Malware Analysis and reverse, Digital Forensics, Sandbox bypass, Shellcoding, Testing Overflows and Exploitation, Code corruption, Testing unexpected behavior, Privilege Escalation, Cryptography, Cryptanalysis, Data infection analysis, new attack vectors, approaches including new tactics and strategies. Defeating protections, intrusion methodologies, polymorphic and intelligent masquerading. Antivirus adaptation and detection avoidance. Development of Tools and scripts.
Web: www.rifec.com | Email: msembiante@rifec.com.

With Every Business a Target for a Security Attack, are Organisations Finally Grasping the Security and Data Protection Nettle or is the Issue Still Being Kicked Into the Long Grass?

I have just had a very busy week. Security flaws were found in a major IT system prior to launch which was duly taken offline and a more secure temporary solution implemented and rolled out in double quick time. Fortunately there was no business or data protection impact, and we even managed to score a pyrrhic victory by getting the vendor to admit that this issue was indeed an issue, and they have gone away to think about solving it. I suspect though that the offending piece of software will ultimately end up as abandon-ware as the cost of really fixing it properly will be so prohibitive that the vendor will be forced to pass the costs on to the customer base, making the project financially unsupportable. Sadly, it was only a matter of time. Our IT department had valiantly raised our heads above the parapet on many occasions about issues with this particular vendor, but due to internal politics it was decided to carry on regardless. Finally the penny dropped, and it looks like a more appropriate technical solution may be rolled out sometime in the future. One for instance that will have a decent API, something that the vendor in question refused to provide as it was not in their commercial interests. They would far prefer to supply a proprietary integration solution at a cost of tens if not hundreds of thousands.

While I am happy that this issue is now being addressed, it is by no means a victory. It wasn't until the weight of evidence was so overwhelming that the decision was taken, and so much pain could have been avoided if the professional opinion of IT had been respected in the first place. The problem comes back to the classic disconnect between IT and management – and the army of departments that want to live in their own little silo with technological autonomy. This is the danger when complex devices and systems are marketed in the same way as block box disposable consumer goods. Nobody wants to think about what goes on under the hood, and those that support and manage these systems are often regarded more as technicians than engineers.

In reality, the word engineer is derived from the Latin ingeniare ("to contrive, devise") and ingenium ("cleverness"). The word technician is a modern construct. To start with, there is a lot of professional jealousy – often on the part of formally qualified engineers – when IT adopts the word "engineer" rather than "technician". Woe betide the skilled programmer or developer who has not got a technical qualification to their name adopting the title "Software engineer". This professional snobbery extends through the management layers, often with the mantra "Paper qualifications good – experience alone bad". The most acclaimed and innovative piece of engineering in human history – the wheel – was invented at the latest between 6500 and 8500 years ago. There is no record of the inventor's gender, but I doubt if they had any professional or educational qualifications to their name.

No, the problem lies in the formalised, metricated, quantified, and qualified society we live in. There is no longer any creative space for the innovator, the idealist, the visionary or common sense unless of course they are willing to work within the strict confines of finance, regulation, management, censorship, or control. That is why whistleblowers and creatives are in such short supply. If you have the right position (i.e. one with clout), you can apparently defy the laws of the universe – but only for a short while until you are found out. Then the PR mantra of "Lessons learned" and a "One off incident" are wheeled out, unless of course the regulator or the justice system bites and then you are really in trouble. The Information Commissioner's Office (ICO) has fined the charity British Pregnancy Advice Service £200,000 for exposing personal data to a malicious hacker via their outsourced website. While I have a great deal of sympathy for the apparent injustice of a charity being fined for a data protection breach, the disconnect is obvious. The trustees placed their trust in a third party who had no real loyalty to the organisation other than to provide a website, and knowing the extreme financial pressures placed on charities and the public sector, there would have been a very tight budget. So no room for penetration testing, a code audit or probably even a decent specification that took into account the data protection risks in such a politically charged arena. The BPA management team will have a harsh lesson to learn on pushing the envelope. IT professionals have no such latitude. Systems are ruthless, almost psychotic in their level of un-forgivenesses. A full stop in a wrong place in a line of code, an unreliable piece of hardware or a badly written specification document can wreak havoc. Never mind deeper logical issues, system complexity, and the hundred and one other pressures that the poor "technician" has to deal with. Good IT people develop a sort of sixth sense over time – call it intuition or whatever – that alerts them to danger. I continually have my leg pulled by colleagues at work because all my servers are backed up daily and every so often I check that the backups are valid. I will not take risks unless I have a plan B and preferably a plan C and D as well. So I go home at night, put my head on the pillow and sleep soundly. What gives me nightmares though is the disconnect between senior management and the technologists – especially where you have a department in the middle that demands their own 3rd party system – and get it. My IT sixth sense knows that the true cost of that system – fully supported, patched and maintained – will be way above the negotiated and signed contract that is eventually agreed upon. So we have IT by committee, built to a price with excellence and worse case – best practice tomorrow. And when the wheel comes off, IT will be will be the first port of call to support a system as after all we are only "technicians" and surely it can't be that complicated to fix. It is no wonder that in IT departments up and down the land, staff have major difficulty in resisting the urge to display banners above their desk that say "I told you so". Hopefully the tide is changing. Organisations are beginning to understand. My engineer manager friend (who is convinced I am a technician) bemoans the lack of "engineers" and freely admits that this is due to lack of candidates willing to work for peanuts. Yes, the downward pressure on salaries is a short term problem, but the bigger long term problem is the cultural divide. Maybe if a few CEO's and CTO's sat down with their IT departments over a beer there would be less potential room for corporate embarrassment.

ROB SOMERVILLE

Rob Somerville has been passionate about technology since his early teens. A keen advocate of open systems since the mid-eighties, he has worked in many corporate sectors including finance, automotive, airlines, government and media in a variety of roles from technical support, system administrator, developer, systems integrator and IT manager. He has moved on from CP/M and nixie tubes but keeps a soldering iron handy just in case.

High-Density iXsystems Servers powered by the Intel® Xeon® Processor E5-2600 Family and Intel® C600 series chipset can pack up to 768GB of RAM into 1U of rack space or up to 8 processors - with up to 128 threads - in 2U.

On-board 10 Gigabit Ethernet and Infiniband for Greater Throughput in less Rack Space.

Servers from iXsystems based on the Intel® Xeon® Processor E5-2600 Family feature high-throughput connections on the motherboard, saving critical expansion space. The Intel® C600 Series chipset supports up to 384GB of RAM per processor, allowing performance in a single server to reach new heights. This ensures that you're not paying for more than you need to achieve the performance you want.

The iXR-1204 +10G features dual onboard 10GigE + dual onboard 1GigE network controllers, up to 768GB of RAM and dual Intel® Xeon® Processors E5-2600 Family, freeing up critical expansion card space for application-specific hardware. The uncompromised performance and flexibility of the iXR-1204 +10G makes it suitable for clustering, high-traffic webservers, virtualization, and cloud computing applications - anywhere you need the most resources available.

For even greater performance density, the iXR-22X4IB squeezes four server nodes into two units of rack space, each with dual Intel® Xeon® Processors E5-2600 Family, up to 256GB of RAM, and an on-board Mellanox® ConnectX QDR 40Gbp/s Infiniband w/QSFP Connector. The iXR-22X4IB is perfect for high-powered computing, virtualization, or business intelligence applications that require the computing power of the Intel® Xeon® Processor E5-2600 Family and the high throughput of Infiniband.

HIGH Throughput & INCREDIBLE Performance Density

IXR-1204+10G: **10GbE On-Board**

4 Server Nodes in 2U

IXR-22X4IB

Intel, the Intel logo, and Xeon Inside are trademarks or registered trademarks of Intel Corporation in the U.S. and other countries.

Call iXsystems toll free or visit our website today! **1-855-GREP-4-IX | www.iXsystems.com**