Gentoo – Zoneminder

The Zoneminder ebuild in the portage tree has been broken for a couple of years now. Here is the process I use to build Zoneminder from source on a Gentoo x86 install:

1. Get Root Access

2. Make The Source Directory

3. Get The Source Package

Stable: *1.25.0*

Development: *svn*

4. Unpack The Sources

5. Install Required Dependencies

Add the following to /etc/portage/package.keywords:

Emerge all dependencies:

Install Sys::Mmap with cpan:

6. Configure and Build Zoneminder

Configure the sources (note this is for a localhost install, you can change it to whatever vhost you want)

Make sure to change the zm db username and password to reflect your setup.

Setup the DB

Import the Initial DB

Build it

After all that Zoneminder should be installed on your system and ready to run. Here are is an init script that I created to get Zoneminder started, stopped and reset as well as allow it to start up and shutdown on a machine power cycle.

Save the file as zoneminder and copy it to /etc/init.d/zoneminder then make sure to run

Now you can start and stop your server by doing:

If you want it to start on power up add it to the default runlevel

Thats it! You should now be able to access the Zoneminder web interface at http://serverip/zm.

Now go buy some cameras!

AsteriskNow – IPTables Firewall Configuration

In a previous guide I discussed how to setup an AsteriskNow server with Polycom phone support. In this guide I will illustrate how to tighten up your server's security by using

the IPTables firewall already installed in the distribution.

IPTables should already be setup and running on the server, however no rules have been applied. You can verify this by doing the following as the root user:

This should report the following:

Verify there are no rules present:

You should see:

Now it’s time to add some rules. You can copy the following text to a file and import it into IPTables:

Save the file as iptables.bak and copy it to /etc/iptables.bak

Now import the file into IPTables:

And verify that the rules have been committed:

You should now see:

Now save the new IPTables settings:

That’s it! Your server is now blocking all incoming traffic by default, and only allowing connections to the ports that are necessary to do it’s job. Specifically:

Port 123 UDP for NTP (Time)
Port 69 UDP for TFTP (Phone provisioning)
Port 5060 UDP for SIP (Phone Calls)
Port 10000-20000 UDP for RTP (Phone Calls)
Port 22 TCP for SSH (SSH Connection)

Port 80 & 443 TCP for HTTP/HTTPS (Web)

If you need to open another port just use the following syntax at the command line:

example for SSH over TCP port 22

To specify a range of ports do the following:

example for RTP over UDP ports 10000-20000

You can then save the new configuration by doing:

And if your completely satisfied and want to back up the configuration do:

Linux – ISO Images

ISO images are very easy to manipulate at the command line in Linux. To make an ISO image from a CD or DVD simply insert the disc into the drive and type:

This uses the dd command with the input set to /dev/cdrom and the output set to filename.iso. Change these values as necessary. Note that some Linux distros mount the cdrom drive to /media/cdrom.

To mount an ISO image and read it just as it was a CDROM loaded in the tray do the following:

The contents of the ISO can now be accessed in /mnt/iso.

AsteriskNow – Polycom SoundPoint IP 335 & 550 Provisioning In FreePBX

AsteriskNow is a free and powerful turnkey open source PBX system that can be combined with high quality Polycom phones to create an enterprise level VoiP solution. In this guide I will outline the steps needed in order to install AsteriskNow and setup automatic configuration and firmware provisioning for your Polycom SoundPoint IP 335 and 550 SIP phones.

Polycom SoundPoint IP 335	Polycom SoundPoint IP 550
	

The first step is to download the ISO image from here. Choose 32 bit or 64 bit depending on the hardware your installing on. Burn the ISO to a CD then boot the computer. You should then see the following screen:

Type 1 and press Enter to install Asterisk 1.6 with the

FreePBX gui.

The installer will begin to load and if the hard disk has not been formatted yet it will ask if you would like to initialze the hard drive. Choose **Yes**. You will then see a screen that gives you partitioning options for your hard drive. If you are only using this computer for AsteriskNow then choose: **“Remove all partitions on selected drives and create default layout”**. Click next, then click Yes when it asks: “Are sure you want to do this”.

Choose your region and click next:

Then set the root password, click next and wait for the installation to complete. Once the installer completes press Reboot and remove the CD from the drive.

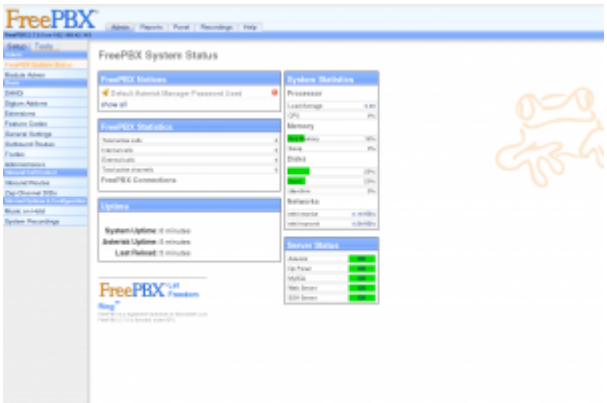
When the machine comes back up you will be presented with the Setup Agent menu. You can use this tool to configure your

network interface card if you need to supply a static IP address. For now we will assume DHCP and just let it time out or exit to proceed. You can call up the network setup utility at any time later and add a static IP, configure the hostname, or add DNS entries by using the command:

The system should now be at a login prompt. Log in as the user root with the password you setup during the installation. Now it is time to update the system with the most current software.

This command will download all of the latest software updates and then ask you if you want to install them. Type y during any prompts. Once the updates are complete reboot your computer by issuing the command:

After the server comes back up from the reboot you will see the login prompt. Above the prompt there should be a line that tells you where to point your web browser to configure AsteriskNow with FreePBX. Point your web browser to the address, click on the **FreePBX Administration** link, and log in with the user **freepbx** and the password **fpbx**. You should now see the FreePBX Status Page.



Now for security purposes we need to change the admin user's password. This will also prevent you from being locked out after we upgrade FreePBX, since for some reason the freepbx user becomes inaccessible after the upgrade. To do this click

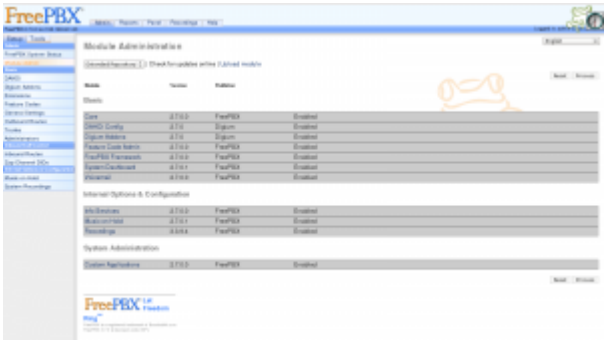
on the **Administrators** link in the Setup menu. You will see a small list in the top left, one button says **Add User** and the other says **admin**. Click on **admin** then change the password in the password box and hit **Submit Changes**.

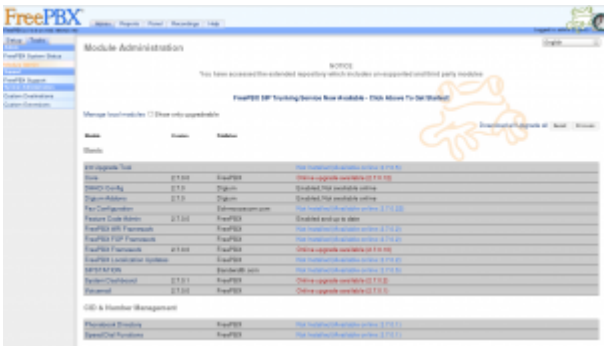
Notice the orange button that now appears on top of the page. You need to click that every time you make a configuration change so that the change can be committed to the system, and Asterisk can be reloaded so the changes can take effect.

Now you can log out and log back in as admin with your new password. Use this account to log in from now on instead of the freepbx user.

Now it is time to update FreePBX from 2.7 to 2.9. There are a few steps to this and they **must** be performed in the correct order. If you are doing this installation in a Virtual Machine I highly suggest you make a snapshot now that you can revert back to if something goes wrong. If you don’t know what a Virtual Machine is then just disregard that last statement!

To upgrade FreePBX select **Module Admin** from the Setup menu. In the drop down box select **extended repository**, click Ok on the prompt then click on **Check for updates online**.





You will now see a list of packages, some of them will be marked with an available update, and some will be marked as not installed. The only package we are concerned with at the moment is the **2.8 Upgrade Tool**. Click on it and then select **Download and Install**. Then click on **Process**.

Confirm the installation, click return when the orange box pops up, then click the orange **Apply Configuration Changes** button at the top. Another orange box will pop up, click **Continue with reload**.

You will now have a new menu item in the **Setup** menu called **2.8 Upgrade Tool**. Click on it to use the upgrade tool.

Follow the instructions on the page **TO THE LETTER**!. First you will press the **Upgrade Now** button on the page to update the database. Then you will go back over to the module admin page, click on check for updates online, and ONLY UPDATE the FreePBX Framework module. After the FreePBX Framework is updated select extended repository from the drop down list and check for updates online again. This time click on the **Upgrade All** link to select all modules that need to be updated, change the **2.9 Upgrade tool** to **“No Action”**, and then click **process**. Apply the configuration changes and reload.

Now we can proceed to the 2.9 Upgrade which is basically the same exact process as the 2.8 upgrade except we need to install a few dependency modules first. In the module admin click on check for updates online then select the following 2 modules and set them to **“Download and Install”**:

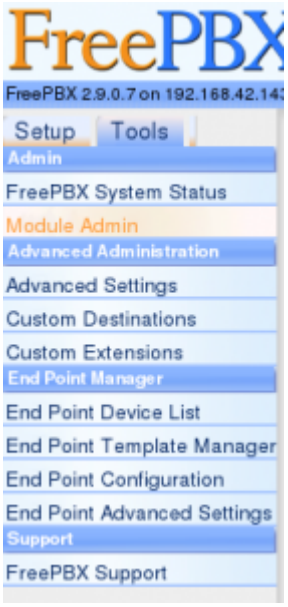
FreePBX ARI Framework
FreePBX FOP Framework

After they are installed apply the configuration changes and reload Asterisk. Then in module admin click check for updates online again, select the 2.9 Upgrade Tool and choose **“Download**

and Install”, then click on **process** to install it. When it is finished installing apply the configuration changes and reload. Then select **2.9 Upgrade Tool** from the Setup menu.

Follow the instructions on the page **TO THE LETTER**!. First you will press the **Upgrade Now** button on the page to update the database. Then you will go back over to the module admin page, click on check for updates online, and ONLY UPDATE the FreePBX Framework module. After the FreePBX Framework is updated select the basic and extended repositories, and check for updates online again. This time click on the **Upgrade All** link to select all modules that need to be updated, and then click **process**. Apply the configuration changes and reload. Now make sure the basic and exended repositories are selected and check for updates online again. Choose **Upgrade All** and then click process. Once it is finished updating the modules apply the changes and reload. Your system should now be fully updated to FreePBX 2.9. Now we can install the Endpoint Manager module that will be used to setup our Polycom phones.

In the module admin make sure the basic and extended repositories are selected then click check for updates online. Now scroll down the list a bit and look for the Endpoint Manager section. Click on **PBX End Point Manager** and choose **“Download and Install”** then click on **process**. Apply the configuration changes and reload Asterisk. You should now have a few **End Point Manager** links in your tools menu.



Now it is time to take a step back from the FreePBX interface and get our hands dirty at the command line! We need to setup and install a few utilities that will be used by the End Point manager to configure the phones. Specifically we need to install nmap, and configure a tftp server that the phones will use to download their configurations and firmware from. We will also need to setup an NTP server that the phones will synchronize their time with.

In a terminal on the AsteriskNow server do the following as the root user:

First install NMAP, type y for any prompts:

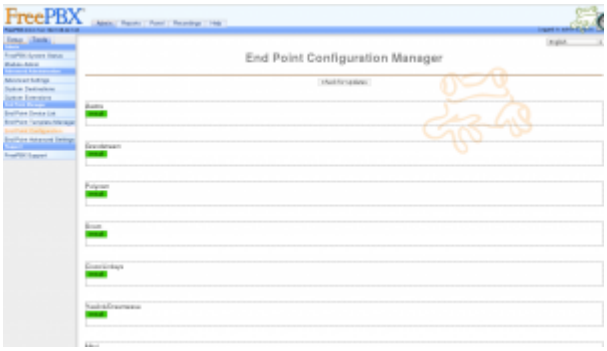
That was easy! Ok now we need to configure a NTP time server, the package is already installed but the service is not running. To start it up and set it to autostart on boot type the following:

Now let’s setup the tftp server:

Thats it for the command line! You can now exit out of the terminal and log back into the FreePBX web interface. Next we will configure the End Point Manager so that it can support the Polycom phones.

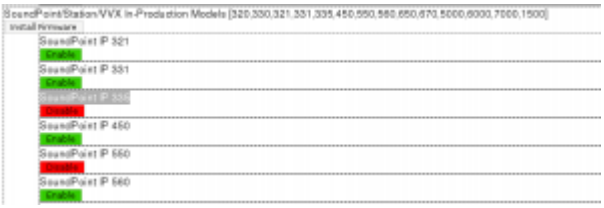
Click on the **Tools** menu then click **End Point Manager Advanced Settings**. Click the **Determine for me** link next to the **IP address of phone server** box. Then make sure the NMAP executable path is set to /usr/bin/nmap. Then click on the **Update Globals** button.

Next click on the **End Point Configuration** link. Then click the **Check for Updates** button, you should now see a list of company names.

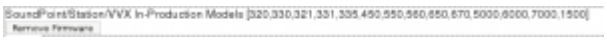


Now click the green **install** button under the **Polycom** section to download configuration files for all of the supported polycom phones.

Now click the green **Enable** button under the **SoundPoint IP 335** and **SoundPoint IP 550** listings to enable them to be used when configuring an endpoint.



Now we need to install the firmware for the PolyCom phones to the /tftpboot folder. This is done by clicking the **Install Firmware** button under the **SoundPoint/Station/VVX In-Production Models [320,330,321,331,335,450,550,560,650,670,5000,6000,7000,1500]** heading. This process will take a few moments to download the files.

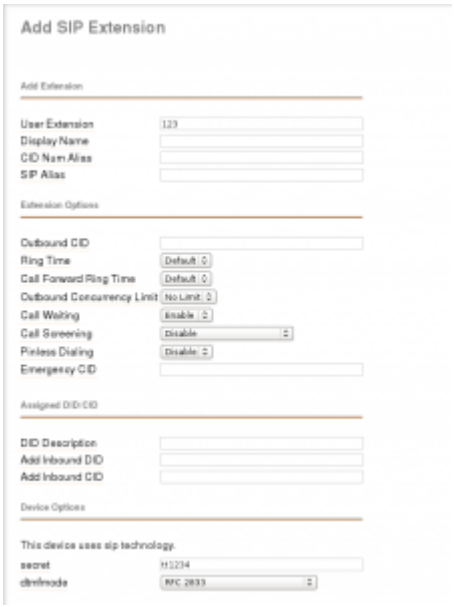


Now we need to create a SIP extension that we can bind a phone to. Click on the **Setup** menu then choose **Extensions** and then choose **Generic SIP Device** in the drop down box. For now lets just get the extension working and not worry about any of the other settings. Enter in information for the following variables:

User Extension

Display Name
secret

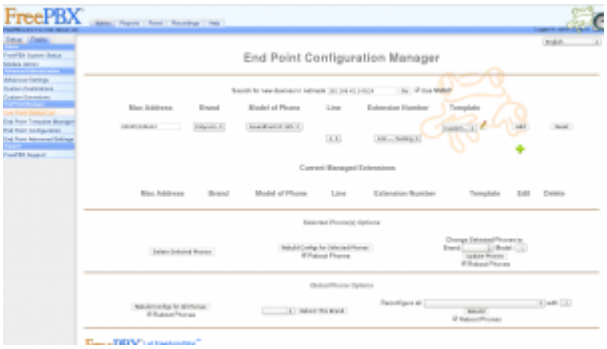
Then apply the configuration changes and reload Asterisk.



Next click on the newly created extension in the list on the right hand side and change the **nat** value to **Yes**.

Now let’s configure an End Point device that will be assigned to this extension. Click on the **Tools** menu and then **End Point Device List**. Enter the MAC Address of the phone (usually located on the bottom), select the brand from the drop down list (Polycom), use line 1, select the extension you just

created, then click the **Add** button.



Thats it for the End Point Configuration. All that is left to now is setup the phone's boot server option to point to the IP address of the AsteriskNow server.

Power up your PolyCom phone enter the setup menu and use the password **456** when prompted. Make sure **DHCP** is set to **enabled** and in the **DHCP Menu** the **Boot Server** option is set to **Custom+Opt.66**. Next in the **Server Menu** make sure the **Server Type** is set to **TrivialFTP** then set the **Server Address** option to the IP address of your AsteriskNow server. Once this is all set reboot the phone and it should connect to the server, synchronize it's time, download and install the new firmware files, and update it's configuration with the extension settings.

To setup more phones just create more extensions and corresponding devices in the End Point Manager. Then setup the phone boot options and you should be good to go!

Xen Cloud Platform (XCP) – Cloning Hard Drive Woes

The main hard drive seems to be flaky in one of my XCP

servers. I decided to use Clonezilla to clone sda to another drive to see if it is in fact the hard drive. After cloning over the drive I found that my LVM storage group VG_XenStorage-xxx was not mounting, and XenCenter was giving off the following error when trying to connect to the server: **“This server cannot see any storage”**

Turns out the LVM volume group was inconsistent after the clone, my guess is because the hard drives were of the same capacity but different brands so there may have been some differences. Using the lvs and vgs commands did not show the LVM volume information, but instead displayed a kernel dump with a plethora of information. The main error being about the inconsistency of the volume group. In order to solve the problem I had to perform the following command:

Then restart the xapi service:

Time to see if we can make it crash again with the new drive!

Gentoo – Framebuffer Splash Image

If you are tired of staring at a black console screen on your Gentoo box you can trick it out a bit using Gensplash. Gensplash or “fbcondecor” allows you to use different background images, fonts and colors to decorate your console so you don’t have the standard black background and white text. It also allows you to have nice boot and shutdown screens. (Think of the boot process and console on the install CD).

First we have to configure the kernel to support the framebuffer devices. You will need the following options enabled in your kernel config:

Next we need to setup some use flags in /etc/portage/package.use:

Then we need to unmask and install the necessary packages:

Now start the fbcondecor service and add it to the default runlevel:

Then create an initrid image and add it’s entry to grub.conf. Note: themes are located in /etc/splash.

grub.conf example:

Grub Notes:

- splash=verbose – means you will see text scroll by, set to silent to just see a fancy progress bar. (Depends on theme)
- fadein – will fade into the framebuffer on boot
- theme:theme_name – the theme you are using
- video=vesafb:mtrr:3,ywrap – vesa framebuffer options
- vga=0x361 – The resolution supported by your video card in hex. Set to Auto to see a list of supported resolutions and their codes for your monitor, experiment, then set it to the one that works.
- CONSOLE=/dev/tty1 – what console do we start the framebuffer on

Reboot and behold the wonders of your new framebuffer!

Gentoo – Deny Hosts

If you find your ssh server is getting hit by a lot of brute force attempts from the internet, and want to do something to defend yourself against them then denyhosts is for you! It helps to alleviate some of the stress on your server that occurs when someone or lots of someones are trying to hack their way into your ssh server. Basically the service watches your ssh traffic, and if it sees an IP address hitting a threshold of failed attempts it adds the address to your /etc/hosts.deny file so that it is blocked from future access attempts.

Simply install the package through emerge:

The initial configuration in /etc/denyhosts.conf should suffice, however it is well commented and you can edit it to suit your needs. You may want to add your email address in the ADMIN_EMAIL = variable so that denyhosts can email you alerts.

Once it is installed and configured start it up and add it to the default runlevel:

Thats it! Your server will now block an IP address after 3 failed ssh login attempts.

But what do I do if I accidentally lock out a valid IP address? Glad you asked!

You need to remove the wrongfully accused IP address from the following files using this process:

First stop the denyhosts service:

Then remove the IP from the following files:

/etc/hosts.deny
/var/lib/denyhosts/hosts
/var/lib/denyhosts/hosts-restricted
/var/lib/denyhosts/hosts-root
/var/lib/denyhosts/hosts-valid

Now restart the service:

You should now be able to ssh from the blocked IP address once again.

Bash – File Backup Script

This script uses rdiff-backup to backup files on a Linux host using rysnc. The script then sends an email that notifies of it's completion. Make sure to install the rdiff-backup package on your distro before running it.

Script Notes:

The script uses a nice value of -19 so that it does not interfere too much with other running processes since file copying is a fairly taxing IO process. Also passing the –exclude flag to rdiff-backup allows you to exclude certain directories from being backed up, such as LOST+FOUND.

Bash – Dynamic Public IP Address Monitor Script

This is a script I wrote to monitor my public IP address to see if it changes or not. It comes in very handy if you run a server on a dynamic IP address. It is setup to run in a daily cron job every morning. The script sends an email that lets me know if the IP address has changed or not, and also reports the current public IP address. Note that this script requires that curl is installed.

Bash – MySQL Backup Script

Looking for a script to backup your MySQL databases on a Linux host? Here is a simple bash script that can be used to automate the process in a cron job. The script checks the database integrity then dumps the database to a text file, tar’s it up, and the emails a confirmation of completion.