

Configuring Your UltraLite Business Server

Configuring Your UltraLite Business Server	1
Setting up your VM environment	2
Logging in to your Virtual Machine	3
Changing the root password.....	3
Changing you IP address	4
Rebooting your Virtual Machine	6
Setting up Kolab for your domain	7
Modify the Hosts File	7
Binding Kolab server to an IP address.....	8
Setting up your domain in Kolab	9
logging into Kolab and Horde interface.....	13
Setup LAMP Apache	13
Start LAMP Apache Server	14
Setup phpLDAPadmin	14
logging into Webmin	15
Setting up phpMyAdmin and changing the default login password.....	15
Setting up Openfire	15
Setting up SparkWeb (Web based client for OpenFire)	16
Setting up Project Pier	17
Setting up Joomla.....	17
Setting up Phreebooks.....	17
Setting up SugarCRM.....	18
Setting up Egroupware.....	18
Setting up Orange HRM	19

Thanks for trying this great server. I have been using it for some time and I am quite impressed with its ability and stability. Please take some time to review the Kolab.org website for more information and tips for getting the most out of your server. Also many thanks to the Kolab group for giving us a great product to use.

Prerequisites:

This server is intended for those who are network administrators, system admins or other computer literate folks. Even if you have worked exclusively with Windows you still should be able to have this server up and running quickly. You should have a basic understanding of IP address, DNS and can find your way through a set of instructions. I believe that anyone can get the mail server up and running in less than an hour, and the Business server in less than two, but you will also need to know how to integrate it into your network and what ports to open on your firewall etc. It is also recommended that you familiarize yourself with VMware in that it is a necessary component of the installation and operation of this server. If you are not familiar with these concepts then this will be a challenge for you and I suggest you hire a network professional to assist you in your implementation.

Credit where it is due:

Kolab and CentOS are both Open Source free products. I just took what others have done, read the documentation, asked friends questions and figured out how to make it work. In the case of the email server I am passing this on for free as my part of the contribution. In the case of the UltraLite Business Server I am charging for the time and effort to get all of the applications up and running in a stable LAMP environment. I am not charging for the software.

Before you start:

Write down the **domain** you are going to be using for email and the **internal IP** address you will be using for the email server as well as the password you would like to use. We will reference this information quite often during the process and writing it down will reduce errors.

UL Business Users: You will need a **second available IP address** for the other services for the configuration of the ULBS server. If that is the case please also note that **IP address** as well. I will refer to the first IP as the eth0 IP address and the second as the eth1 IP address.

The default values are: mail.mydomain.com, 192.168.0.10 (and 192.168.0.11 ULBS only) and administrator.

Domain _____

IP Address 1 _____ (for eth0)

IP Address 2 _____ (for eth1)

Password _____

Setting up your VM environment

1. Extract the downloaded .zip file that you downloaded to an appropriate location.

All you need to run the server is the VMware player that you can download from here

<http://www.vmware.com/products/player/>

2. After you have installed VMware Player go to File>Open and browse to the kolab.vmx file that you extracted earlier.

3. Click the green play button on the VMware Player console and your server will begin booting up.

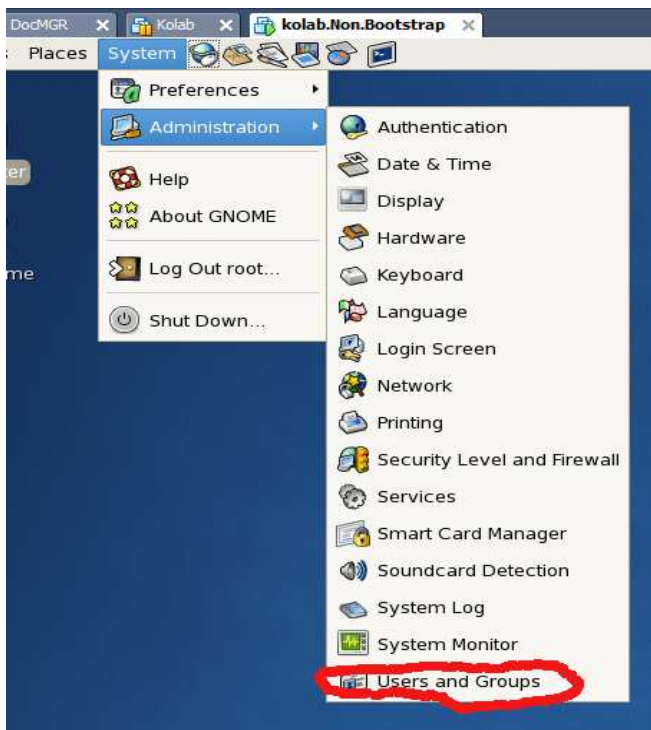
Note: if asked “Copied it or Moved it” choose copied.

Logging in to your Virtual Machine

The login is root and the password is administrator

Changing the root password

1. On the tool bar click on system >administration>users and groups



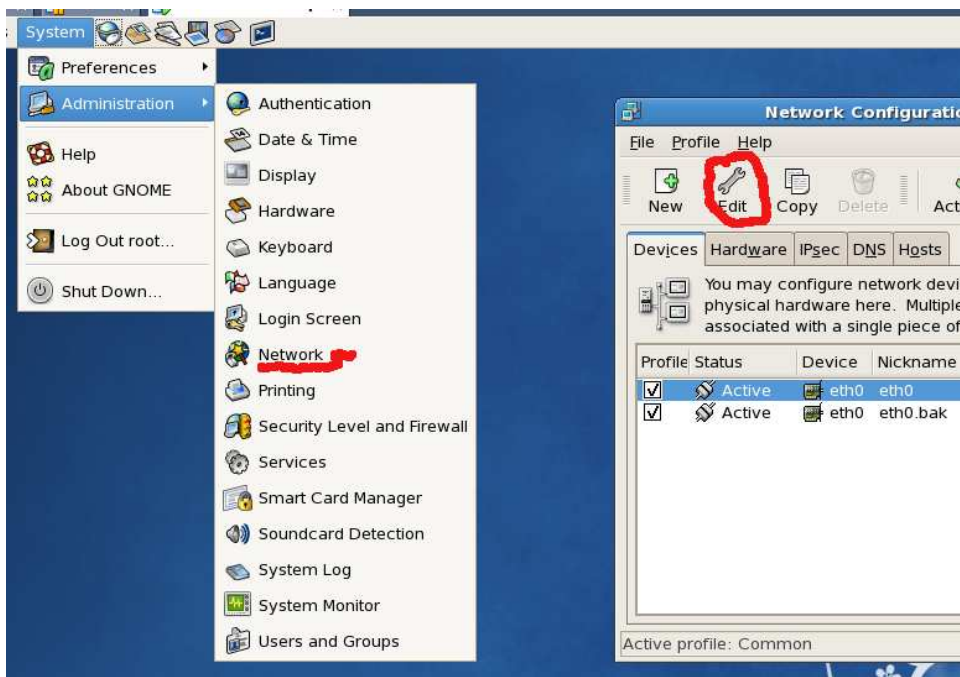
2. Go to Edit>Preferences and uncheck the Hide System Users and Groups box.



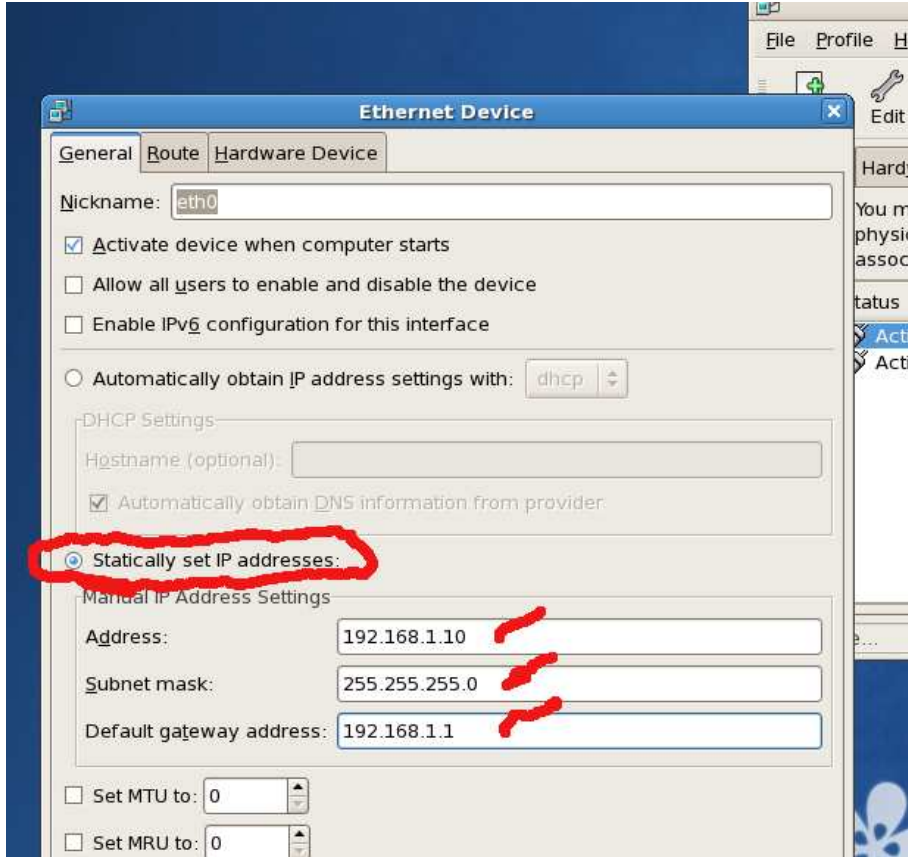
3. Double click root and type in you desired password and confirm it. Click OK and close the User Manager.

Changing you IP address

1. Go to System>Administration>Network and click edit for eth0
 For ULBS you will need to change both the eth0 and the eth1 interface. Use the same process to edit eth1 giving it the second IP you wrote down at the beginning of the process

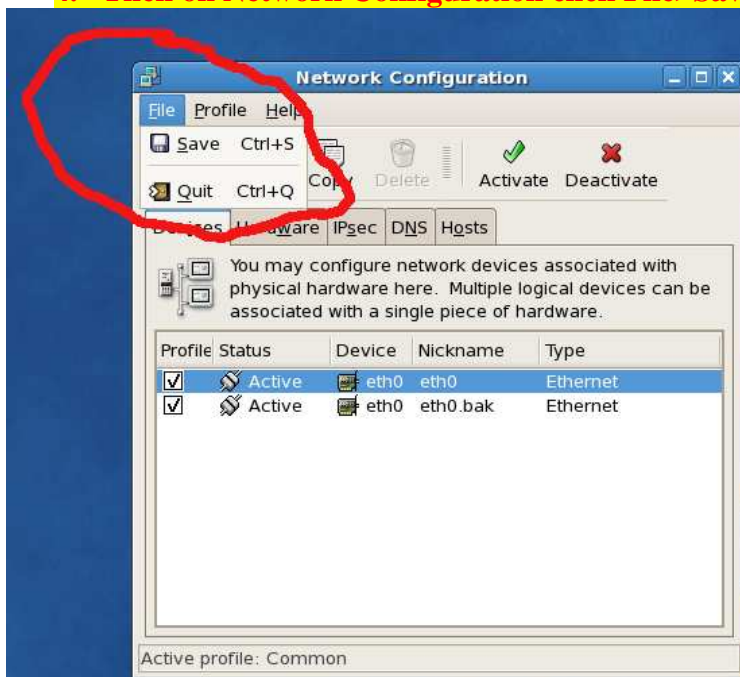


2. Click on the statically set IP address and set it for your IP scheme.



3. Click OK

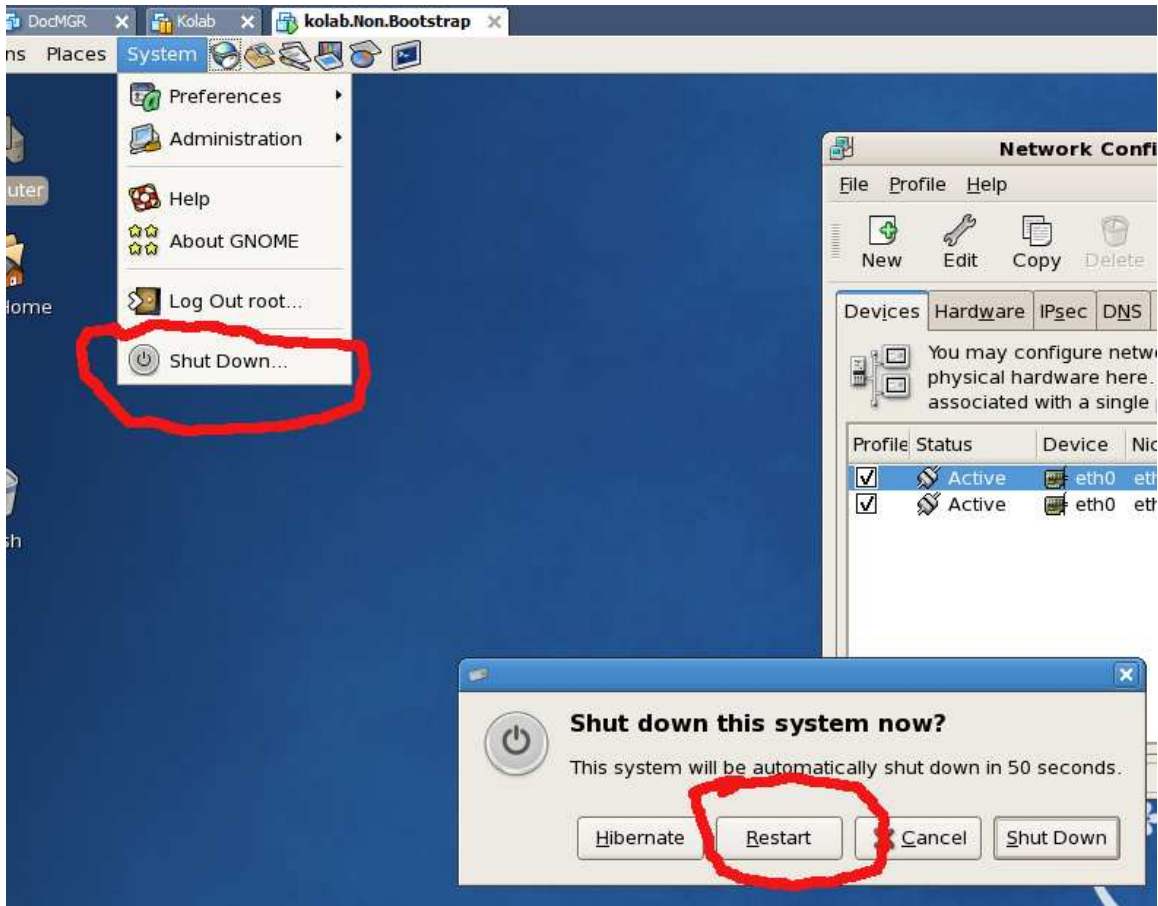
4. Then on Network Configuration click File>Save



5. You will get a screen confirming your change and warning you to restart your network services. Please reboot the Virtual Machine at this point.

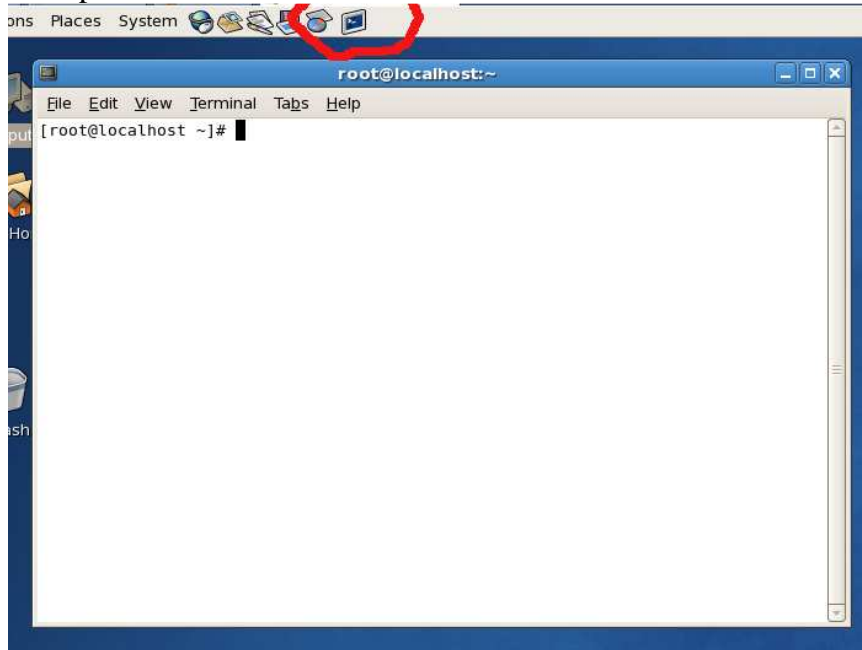
Rebooting your Virtual Machine

Go to System>Shut Down and then chose reboot.



Setting up Kolab for your domain

1. Open a terminal while in CentOS



2. Shut down all services for Kolab by typing `/kolab/bin/openpkg rc all stop`
3. Type in `/kolab/sbin/kolab_bootstrap -b` and answer the questions. They are pretty basic but if you need help go to the Kolab.org site for info.
4. Start up all services for Kolab by typing `/kolab/bin/openpkg rc all start`
5. Close the terminal

Modify the Hosts File

1. This is necessary for name resolution prior to a DNS entry on your network. Don't skip this step or things won't work right during the setup process.
2. Double click on the "link to hosts file on the desktop"
3. Change 192.168.0.10 to your first IP address (the eth0 address)
4. If you are configuring the UltraLite Email server go to section "Setup your Kolab Server"

ULBS users only

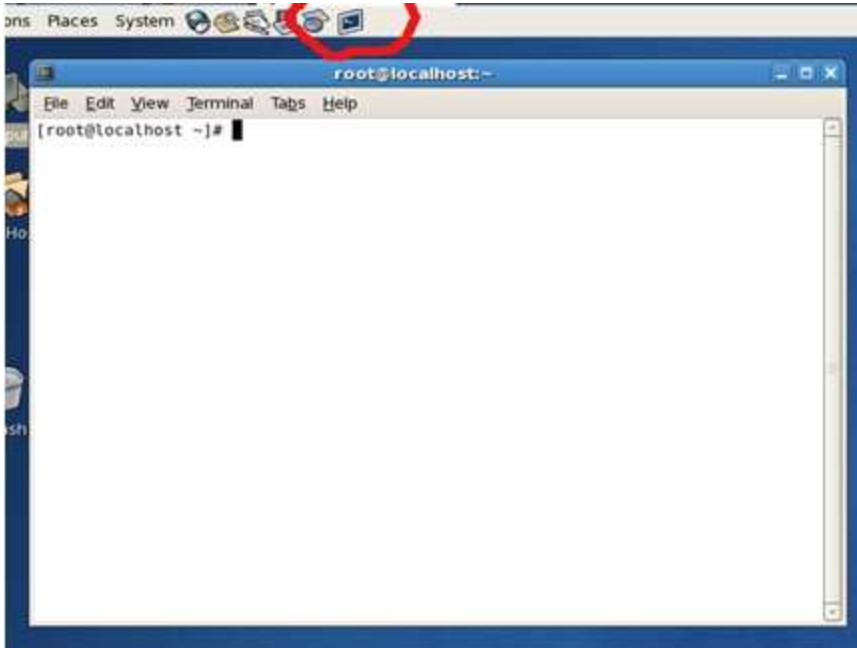
5. Change 19.168.0.11 to your second IP address (the eth1 address)
6. Change the mail.myserver.com to the name of your mail server (ie. mail.systemalternatives.net)

7. Save and Close the file

Binding Kolab server to an IP address.

We are going to bind the Kolab web server to the first IP address (eth0)

1. Open a terminal while in CentOS



2. Start all services for Kolab by typing `/kolab/bin/openpkg rc all start` (You will get an error that apache can't start, don't worry about that for now>)

3. Minimize the terminal

4. Double click on the "Kolab Apache Configuration" Icon on the desktop.

5. Scroll down to line 113 and 114

6. Modify the IP addresses on both lines to match the first address (eth0) you wrote down

7. Save and Close the file

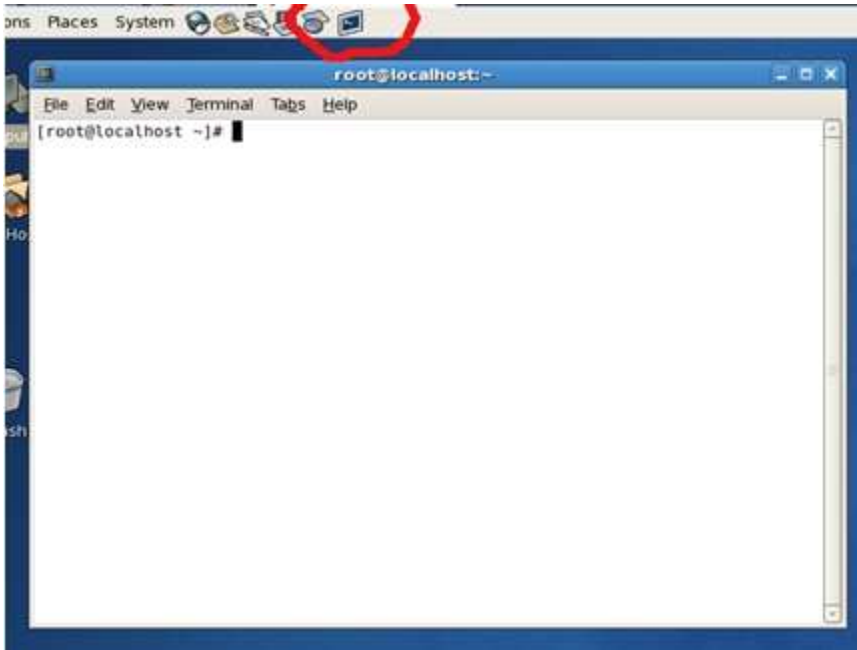
8. Bring up the terminal again and enter `/kolab/sbin/kolabconf`

9. Stop all services for Kolab by typing `/kolab/bin/openpkg rc all stop`

10. Close the terminal

Setting up your domain in Kolab

1. Open a terminal while in CentOS



2. Shut down all services for Kolab by typing `/kolab/bin/openpkg rc all stop`
3. Type in `/kolab/sbin/kolab_bootstrap -b` and answer the questions. *They are pretty basic but if you need help go to the Kolab.org site for info or look at the example I have posted below.*
4. Start up all services for Kolab by typing `/kolab/bin/openpkg rc all start`
5. Close the terminal

Example Bootstrap with Notes:

> means the computer is asking for input

Italics are my notes

Regular text is what the computer is throwing out as we go through the script

1. Input Hostnames

> **Please enter Hostname including Domain Name (e.g. thishost.domain.tld)**

[example]: kolab.example.com

Proceeding with Hostname kolab.example.com

Enter the name of the server probably mail.mydomain.com where mydomain.com is the domain you want for email.

Select Master Server

> **Do you want to set up (1) a master Kolab server or (2) a slave [1]**
(1/2): 1 (always 1)

Proceeding with master server setup

2. Input the mail domain

> **Please enter your Maildomain - if you do not know your mail domain use the fqdn from above [yourdomain, no brackets!]: [Enter]**

(enter the domain that you want this server to receive mail for)

proceeding with Maildomain example.com

Kolab primary email addresses will be of the type user@example.com

Generating default configuration:

Top level DN for Kolab [dc=example,dc=com]:

base_dn : dc=example,dc=com

bind_dn : cn=manager,cn=internal,dc=example,dc=com

3. Setting the manager password

> **Please choose a manager password [your password with no brackets!]: [Enter]**

This will be the administration password for the Kolab web interface.... Don't loose it!

bind_pw : <managerpassword>

done modifying /kolab/etc/kolab/kolab.conf

IMPORTANT NOTE:

use login=manager and passwd=VG1rXCixi22/c4DT when you log into the webinterface!

4. Setting a slave Kolab server

> **Enter fully qualified hostname of slave kolab server e.g. thishost.domain.tld [empty when done]: [Enter]**

(We aren't doing a slave so just leave it blank and hit enter)

prepare LDAP database...

temporarily starting slapd

Waiting for OpenLDAP to start

no dc=example,dc=com object found, creating one

mynetworkinterfaces: 127.0.0.0/8

LDAP setup finished

Create initial config files for postfix, apache, cyrus imap, saslauthd

running /kolab/sbin/kolabconf -n

kill temporary slapd

OpenPKG: stop: openldap.

Creating RSA keypair for resource password encryption

/kolab/bin/openssl genrsa -out /kolab/etc/kolab/res_priv.pem 1024

Generating RSA private key, 1024 bit long modulus

.....++++++

```

.....++++++
e is 65537 (0x10001)
/kolab/bin/openssl rsa -in /kolab/etc/kolab/res_priv.pem -pubout -out
/kolab/etc/kolab/res_pub.pem
writing RSA key
chown kolab:kolab-n /kolab/etc/kolab/res_pub.pem /kolab/etc/kolab/res_priv.pem
Kolab can create and manage a certificate authority that can be used
to create SSL certificates for use within the Kolab environment. You
can choose to skip this section if you already have certificates for
the Kolab server.
5. Create the certificates (for SSL)
> Do you want to create CA and certificates [y] (y/n): y
(Always yes, we want certificates)
Now we need to create a certificate authority (CA) for Kolab and a server
certificate. You will be prompted for a passphrase for the CA.
#####
/kolab/etc/kolab/kolab_ca.sh -newca kolab.example.com
> Enter organization name [Kolab]: [Enter]
(use you company name like systemalt or something like that)
> Enter organizational unit [Test-CA]: [Enter]
(use your companyname-ca like systemalt-ca)
Using subject O=Kolab,OU=Test-CA,CN=kolab.example.com
Using dn
> CA certificate filename (or enter to create) [Enter]
(Just hit enter)
Making CA certificate ...
Generating a 1024 bit RSA private key
....++++++
writing new private key to '/kolab/etc/kolab/ca/private/cakey.pem'
> Enter PEM pass phrase: <passphrase>
(Use any password you wish, just don't forget it!)
> Verifying - Enter PEM pass phrase: <passphrase>
(Verify the password you just entered)
-----
/root
/kolab/etc/kolab/kolab_ca.sh -newkey kolab.example.com /kolab/etc/kolab/key.pem
Using dn
Generating RSA private key, 1024 bit long modulus
.....++++++
e is 65537 (0x10001)
writing RSA key
/root
/kolab/etc/kolab/kolab_ca.sh -newreq kolab.example.com /kolab/etc/kolab/key.pem
/kolab/etc/kolab/newreq.pem
Using dn
Request is in /kolab/etc/kolab/newreq.pem and private key is in /kolab/etc/kolab/key.pem

```

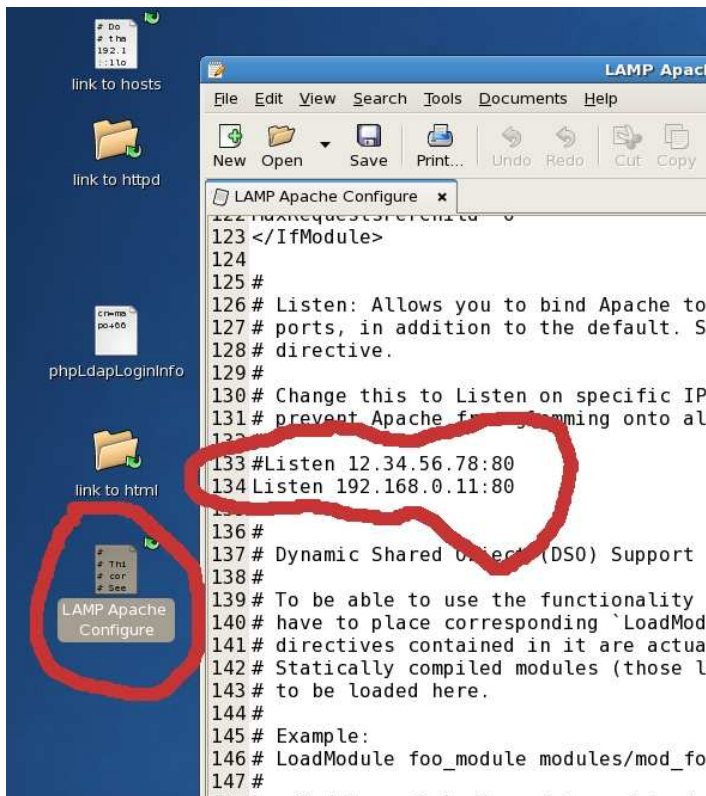
```
/root
/kolab/etc/kolab/kolab_ca.sh -sign /kolab/etc/kolab/newreq.pem
/kolab/etc/kolab/cert.pem
Using dn
Using configuration from /kolab/etc/kolab/kolab-ssl.cnf
> Enter pass phrase for /kolab/etc/kolab/ca/private/cakey.pem: <passphrase>
(Enter that password yet one more time)
Check that the request matches the signature
Signature ok
Certificate Details:
Serial Number: 1 (0x1)
Validity
Not Before: Oct 19 07:24:15 2007 GMT
Not After : Oct 16 07:24:15 2017 GMT
Subject:
commonName = kolab.example.com
X509v3 extensions:
X509v3 Basic Constraints:
CA:FALSE
Netscape Comment:
OpenSSL Generated Certificate
X509v3 Subject Key Identifier:
65:CD:3E:49:47:34:B6:05:52:25:3B:C7:C5:4D:7D:09:92:13:6D:1B
X509v3 Authority Key Identifier:
DirName:/O=Kolab/OU=Test-CA/CN=kolab.example.com
serial:85:3B:73:2D:BA:56:FC:67
> Certificate is to be certified until Oct 16 07:24:15 2017 GMT (3650 days)
Sign the certificate? [y/n]: y
> 1 out of 1 certificate requests certified, commit? [y/n] y
Write out database with 1 new entries
Data Base Updated
Signed certificate is in /kolab/etc/kolab/cert.pem
/root
chgrp kolab-r /kolab/etc/kolab/key.pem;
chmod 0640 /kolab/etc/kolab/key.pem;
chgrp kolab-r /kolab/etc/kolab/cert.pem;
chmod 0640 /kolab/etc/kolab/cert.pem;
#####
CA and certificate creation complete.
You can install /kolab/etc/kolab/ca/cacert.pem on your clients to allow them to verify
the validity of your server certificates.
```

logging into Kolab and Horde interface

1. To access the Administration Console open a web browser and go to <https://theipaddress/admin> confirm the certificate exception and login using the username and password given in the bootstrap process. (ULBS users use the first IP address, the one we bound to eth0)
2. To access the Horde email client open a web browser and go to <https://theipaddress/horde> confirm the certificate exception and login using the username and password created in the administration console. (ULBS users use the first IP address, the one we bound to eth0)
3. For documentation on configuring the mail server go to <http://www.kolab.org/doc/doc2-1.72.pdf> , download the file and go to page 26. You will find all the info on the server admin console there.
4. For managing Horde use the embedded help.

Setup LAMP Apache

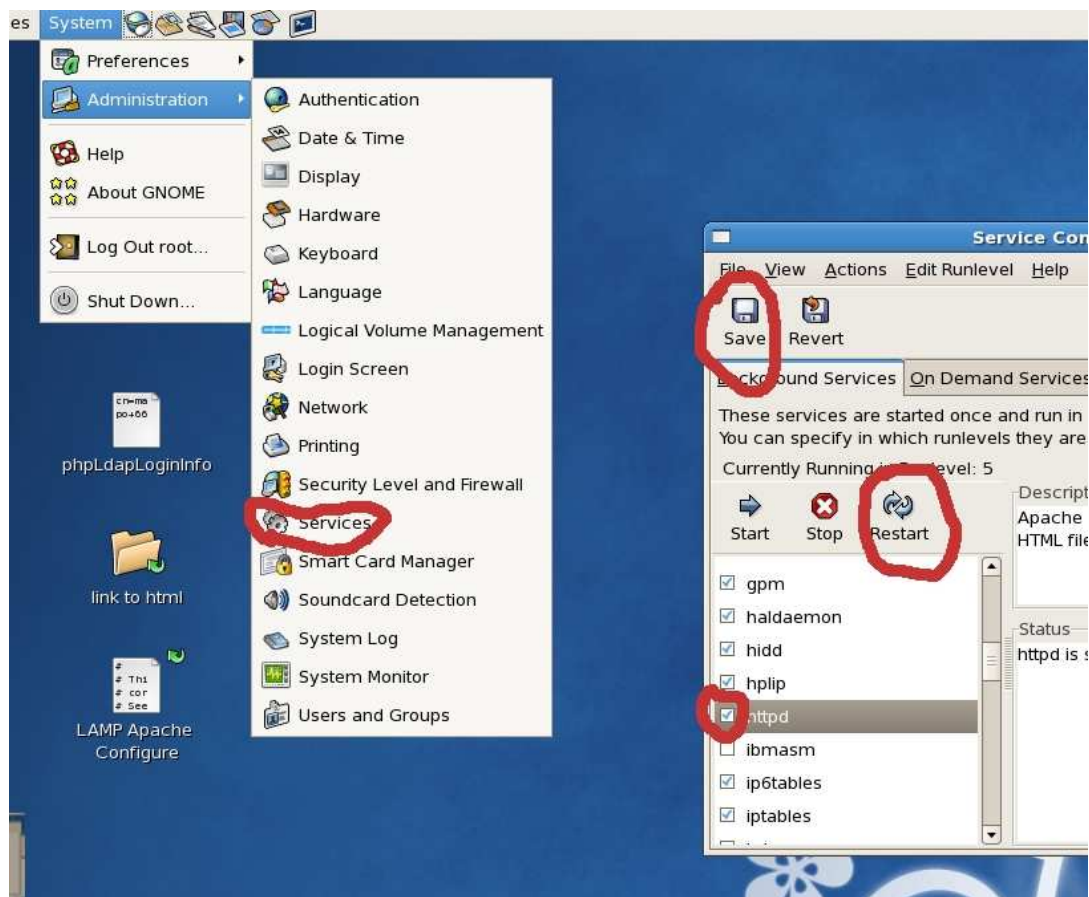
1. Double Click on the Lamp Apache Configuration on the desktop
2. Scroll down to Line 134
3. Modify the IP address to match the second IP address (the eth1 IP address)



4. Save and Close the document

Start LAMP Apache Server

1. Open the service configuration GUI by going to System>Administration>Services
2. Scroll down to the httpd service, select it and check the box if it is not already checked.
3. Click save
4. Click restart



Setup phpLDAPadmin

Setting Up phpLDAPadmin

1. Open your web browser and type `http://pla`
2. For the Login DN use `cn=manager,cn=internal,dc=yourdomain,dc=com`
3. Where *yourdomain* and *com* is the domain you used when you set up your Kolab server.
4. The password is the password you used when you set up the Kolab server.

Note: If you get into trouble getting the username and password correct open the link to the Kolab Configuration on the desktop. The user name is the bind_dn and the password is the bind_pw.

for more information on using phpLDAPadmin visit their website at www.phpldapadmin.org

logging into Webmin

Webmin is a great management tool. It comes with the server. I have done some pre-configuration but you may want to do more. You can read more on Webmin and its capabilities at www.webmin.org

1. log in to Webmin by going to <http://localhost:10000>
2. Username is root
3. Password is the password you wrote down at the beginning

Setting up phpMyAdmin and changing the default login password.

phpMyAdmin is a web based database management system for MySQL. It can be used to manage all of the applications databases (except Kolab) setup on the server. Please visit www.phpmyadmin.org for more on using phpMyAdmin.

Open <http://phpmyadmin> in a web browser

For the first login,

1. Login using username root, the password is administrator.
2. Click on privileges
3. For each user labeled "root"
 1. Click on "edit privileges" icon (the symbol in the far left column)
 2. Scroll down to find the change password section
 3. Enter your password in both the password and re-type sections
 4. click "go"
 5. click on "Privileges" at the top of the page
 6. Repeat for each user named "root"

Note: During the process you may be logged out when you change a password. Log back in using root and the new password.

Setting up Openfire

Openfire is an instant messaging server that is manageable through a web based interface. In order make it work with the Kolab LDAP server the configuration script needs to be run.

1. Open the web browser and go to localhost:9090
2. Accept the default settings for Language Selection, Server Settings and Database settings
3. Under Profile Settings choose Directory Server (LDAP)
4. On the next screen choose
 1. Server Type "Open LDAP"
 2. Leave Host and Port as Default
 3. Base DN `dc=mydomain,dc=com` Where *mydomain* and *com* are the domain name you used for your kolab server
 4. The Administrator DN is `cn=manager,cn=internal,dc=mydomain,dc=com`
 5. Password is your password

Note: If you are having trouble with these entries double click the Kolab Configuration link on the desktop. The base DN is on line 3 and the Administrator DN is on line 4 and the password is on line 5.

5. Click Test Settings to confirm
6. Click Save & Continue
7. On the next page leave the default settings
8. Click Test Settings to confirm
9. Click Save & Continue
10. On the next page leave the default settings
11. Click Test Settings to confirm
12. Click Save & Continue
13. On the Add Administrator screen use Manager for the add administrator entry
 1. Click Add
 2. Click on the test icon (looks like a gear)
 3. Type in your password and click Test
 4. Close the test window and click continue (This will take a few minutes)
14. Login to the Management Console.
15. For information on settings please see the documentation on the web at <http://www.igniterealtime.org/community/index.jspa> Most of the information is intuitive enough. The server is actually ready at this point. Users will need to be setup in the Kolab management console

Note: I include the web based client, pre-installed on this box. You can also use the windows based client called Spark. You can download it from <http://www.igniterealtime.org/projects/spark/index.jsp>

Setting up SparkWeb (Web based client for OpenFire)

1. Open a web browser and go to <http://sparkweb>
2. For username use the username from Kolab (The first part of the email address)
3. For the Server use the first IP address
4. For the password use the users password from Kolab
5. Your in!

Setting up Project Pier

Project Pier is a web based project management tool. It can help you manage multiple projects with many companies and resources.

1. Open the web browser and go to <http://projectpier>
2. Login using admin and administrator
3. Click on Account and then Change password
4. Update the password to your password
5. For information on using and administrating Project Pier go to <http://www.projectpier.org/manual/tour/quickstart>

Setting up Joomla

Joomla is a premier web site content management system. With hundreds of free modules it can be customized for a look and feel that will work great for a company Intranet or even a website.

1. We need to make an update to the Joomla configuration file due to the change in the root password made at the beginning of the configuration.
2. Click the desktop link "Joomla Configuration File"
3. Scroll down to line 17
4. Change the administrator to your new password
5. Open the web browser and go to <http://joomla> to see the web page
6. Open the web browser and go to <http://joomla/administrator> for administration of the site.
7. Login using admin and administrator
8. Go to Site> User Manager
9. Click on the administrator account
10. Enter your new password and verify
11. Click Save and then logout
12. Log back in using the new password
13. For more information on using Joomla go to www.joomla.com

Setting up Phreebooks

Phreebooks is a great web based accounting package featuring cycles for all of the major business functions.

During the setup you will be installing a chart of accounts. I recommend consulting an accountant prior to installation to insure that you have the right accounts in your database for your company.

1. Open the web browser and go to <http://phreebooks/modules/install>

2. Click through the Welcome screen, the License Agreement, and the Prerequisites
3. Click Install at the bottom of the prerequisites screen
4. Leave the system defaults for the System Setup
5. On the Database Setup screen change the database username to phreebooks and the password to administrator
6. Enter phreebooks for the company database name and click next
7. In the Admin setup screen enter and confirm the password and admin account info. I always use Admin for the administrator and my password for the username.
8. The next screen is your company info. The only thing to avoid here is the installation of the Demo Company.
9. Click save company settings when you are done
10. On the Chart of Accounts choose the chart closest to your type of business. (The chart can be modified once install)
11. The rest is self explanatory.
12. For information of the use of the product please visit http://www.phreebooks.com/pb_phpBB/index.php . Also this product has online help that is pretty good.

Setting up SugarCRM

Sugar CRM is one of the leading customer relationship software packages out there with many features that you would find in the pay-for products we all know and love.

1. We need to make an update to the sugarcrm configuration file due to the change in the root password made at the beginning of the configuration.
2. Click the desktop link “SugarCRM Configuration File
3. Scroll down to line 36
4. Change the administrator to your new password
5. Open the web browser and go to <http://sugarcrm>
6. login as admin, administrator
7. Click on Admin (Top towards the right)
8. Scroll down and click on User Management
9. Click on Administrator
10. Click on Change Password, Enter and confirm the new password
11. Logout and back in to confirm the password
12. For additional information on using sugar CRM consult the online help or go to <http://www.sugarcrm.com/university>

Setting up Egroupware

1. Open the web browser and go to <http://egroupware>
2. login as admin, administrator
3. Click on preferences (upper left)

4. Click on Change your Password
5. Click edit
 1. Old password is administrator
 2. Enter and confirm your new password
 3. Logout and log in to confirm
6. For information on how to use Egroupware consult the online Manual/Help or go to http://www.egroupware.org/?category_id=232

Setting up Orange HRM

OrangeHRM is a Human Recourse Management Suite containing all of the popular functions needed to organize a HR department and keep track of employees.

1. Open the web browser and go to <http://orangehrm>
2. Login using admin, administrator
3. Click on Change Password
4. Click edit
 1. Old password is administrator
 2. Enter and confirm your new password
 3. Logout and log in to confirm
5. For more information on Orange HRM please visit <http://www.orangehrm.com/support-plans.php> Under the support plan table you will see a link to the quick start guide.