LOGO

E-mail:
webmaster@ webterse.com
gaurav@ mail.webterse.com
hostmaster@ mail.webterse.com

Blog working! HTTPS enabled using certbot!

- Click to download Webterse websitePDF document. Download link

WebServer and E-mail Server

This website provides details to install WebServer and E-mail Server, Self-Hosted on Laptop connected to Internet via ethernet cable/wireless, having Ubuntu 18.04.2 LTS Server Version Operating System with Open SSH Server selected during Ubuntu installation. It is better to have a Laptop dedicated only for Ubuntu Server Operating System rather than having a second OS (the other OS being Windows Home 8.1/10 with Office Professional Plus 2013(Office15) or vice-versa) alongside selected at time of laptop boot-up, on the same Laptop. You can use rufus on Windows for making bootable USB for Ubuntu 18.04.2 LTS Server from it's downloaded ISO image and boot from USB as first preference in Laptop BIOS setup. Ubuntu Server version does not have a graphical desktop or web browser. It has shell/terminal to run commands.

1. Nginx WebServer

- Nginx version 1.16.0 WebServer configuration serving static pages (to start with) of HTTP Website, accessed typing private/local IPaddress in the web-browser from another Laptop/Mobile phone connected to either same mobile hotspot or same Internet connection as webserver, during development.
- HTTP Website with HTML Sitemap for supporting user navigation, using Microsoft Expression Web 4 editor and template.
- Sitemap (XML file) is used by web crawler to index the website when search engines like google and bing are used, for example, XML Sitemap can be submitted to Google by verifying ownership of your website in Google Search Console and then submit your files to Google.
- Php7.2-fpm for Nginx additionally serving dynamic webpages.
- Php7.2-mysql as connector.
- MySQL 5.7.27 for Database Server using mysql-server_5.7.27-1ubuntu18.04_amd64.deb-bundle. It is important that the MySql server installation should prompt for setting root password during the installation
- WordPress as Content Management System (CMS) and website development (re-install wordpress again after taking static-ip connection).
- Making own blog (Blog) using WordPress (An instance of WordPress can be used make a seperate full-blown commercial website rather than just a blog).
- Making own blog (Blog-coded) using PHP and HTML code, uses php7.2-sqlite as connector and PDO for sqlite as driver.

    - For accessing, click Blog-coded in the menu-bar on webterse.com and type index.php in place of default.html and press Enter.
    - Accessing alternatively as a subdomain that is blog-coded.webterse.com (add to GoDaddy DNS Records, check your DNS Provider FAQs on adding subdomain).

1.1 Registering (Annual Paid Subscription & Renewal) to get a domain name from DNS provider, for example Google domains

- While taking domain, type domain as webterse.com (without www). There will be an automatic CNAME www entry in your domain provider DNS records.
- They give you domain e-mail support with e-mail forwarding included with the bought domain for $12 + taxes (Rupees 862 + taxes).
- Domain-email support means postmaster@bought-domain.com, webmaster@bought-domain.com or admin@bought-domain.com etc.
- You will require domain-email for free Class 1 SSL/TLS bought-domain validation, and it is better to purchase domain with domain-email support included.
- I purchased domain for around Rupees 1050 including taxes for a year from Godaddy, wherein you have to purchase additionally domain-email support for around Rupees 552 + taxes/year, but you may be able to buy a domain for less than $ 12 only-initially for a year from Godaddy as compared to Google domains with included domain-email support

1.2 Making Website HTTPS (Using SSL/TSL Certificate available freely-total/freely-for-few-month(s) and then renewable-on-payment, free providers come-and-go on Internet)

SSL-TLS certificate signed by real Certificate Authority (CA), for example QualitySSL and Let'sEncrypt certbot for use on world-wide-web.

- Domain validation using domain-email correspondence, for free SSL/TSL Class 1 certificate, not having static IP yet from your ISP Internet Service Provider, different free SSL/TLS certificate provider for example QualitySSL.com (30 days) than your bought-domain provider. You may generate CSR Certificate Signing Request at your Nginx webserver terminal and upload CSR with remaining details at the free SSL/TLS certificate provider website, or directly fill all the details for CSR at the free Class 1 SSL/TLS provider website. Manual nginx virtual host file configuration. The SSl-TLS certificate provider will have it's own set of instructions for installing certificate.
    - Generally, key.file (private-key encrypted) and certificate.file (contains public-key) are placed in /etc/nginx/ssl folder.
    - Edit configuration in nginx virtual host file.
    - You can read on arstechnica.com/information-technology/2012/11/securing-your-web-server-with-ssltls/2 or Click here.
- Automated domain validation for free Class 1 SSL/TSL certificate, for example Let'sEncrypt: certbot (90 days, can be renewed every 60 days, renewal is free) having static-IP from your ISP Internet Service Provider.
- Point A record of Godaddy DNS to your-static-ip. There is propagation time before you can access your website using domain name. Run automated certbot execution, in this you have to enter details at the nginx webserver terminal. Certbot runs cron.d service located at /etc/cron.d twice a day on your webserver. You may not want this service to run and hence not use Let'sEncrypt.
- Execute Automated validation for subdomain having it's own virtual host file and document root folder, in a similar way.

1.3 Lastly, taking/activating static-IP from your ISP Internet Service Provider (preferably wired connection), configured with

their router, to make your website publicly accessible everywhere.

- For example, Airtel activates single-static-IP for Rupees 99/month on it's wired broadband connection (upto 40 Mbps plan), on DSL (Telephone) cable line with their modem-cum-router with wifi-interface.
- Your wired broadband ISP will assign you DHCP LAN address range for internal/local use, for example, 192.168.1/24, with available addresses from 192.168.1.2 to 192.168.1.254, 192.168.1.1 being modem-cum-router address and 192.168.1.0 ans 192.168.1.255 being system reserved addresses.
- DHCP automatically assigns a LAN ip address to a client machine(s) on LAN from the DHCP LAN address range. It may/may not change (if isc-dhcp-server is not installed) for a machine if the router is restarted (power outage).
- Your webserver having static-ip address (public-external) will also be having one of the internal DHCP LAN address, for example 192.168.1.2
- You may use a better supporting router afterwards.For example, Cisco RV340, CiscoRV340W (wifi5 interface).
- For example, Mobile Hotspot and Wired Broadband connection, though both can be of Airtel as ISP, but are two different (routes) Internet connections.
- If webserver is on Wired Broadband connection then with respect to wired-broadband-router-with'nwithout-wifi-interface, routes can be thought of as follows:

    - Mobile Hotspot/Mobile Internet/Internet connection different from Webserver: out->in (you use a static-ip)
    - Wired Broadband with'nwithout wifi interface: in->in (you use a DHCP LAN ip)

1.3.1 Before taking static-ip: During development of webserver and website, use either same mobile hotspot or same Internet connection for both, webserver and another Windows laptop/Mobile phone using private-local ip.

- A private-local ip address of a home-Internet-connection/mobile-Internet-connection is not internet routable for the webserver.

1.3.2 SSH into webserver from client: Webserver access after taking static-ip and certbot

- Accessing terminal (using username and password only for SSH, without Key-based authentication): Simply use DHCP-Lan-ip over Putty-for-SSH-on-Windows/SSH-Ubuntu terminal, if you are using either same mobile hotspot or same Internet connection for both, webserver and another laptop. Use static-ip if using a different Internet connection from that of the webserver Internet connection.

    - From another remote Windows laptop use Putty (type static-ip/DHCP-LAN-ip and click connect) or Windows laptop running Virtual Box Ubuntu desktop/server in terminal, type ssh user@DHCP-Lan-ip/static-ip address.
    - From another remote Ubuntu desktop/server, in terminal type ssh user@DHCP-Lan-ip/static-ip address.

- Using username and password with Key-based authentication for SSH:
  - You can read about SSH key-based authentication on help.ubuntu.com/community/SSH/OpenSSH/Keys or Click here.
  - On Windows use puttygen to generate the needed keys for key-based authentication.
  - You will be most secure by protecting your key with a passphrase.
- In etc/ssh/sshd_config type at bottom type AllowUsers user1 user2 user3

1.3.3 SSH or SSHFS into webserver from Ubuntu (VM virtual machine on windows laptop) client machine with key-based authentication (private key, public key) pair, after taking static-ip and certbot.

sshfs is used to mount the webserver directory on the client directory. After successful mount the webserver directory contents can be copied into client machine location. We will also use ssh to login using key-based authentication.

On client machine: from username prompt

- sudo apt-get install sshfs
- mkdir ~/.ssh
- chmod 700 ~/.ssh
- ssh-keygen -t rsa (generate private-public set of keys, ssh-keygen -t rsa -b 4096 for 4096 bit key, default is 2048 bit)
- Enter file in which to save the key (/home/username/.ssh/id_rsa): press Enter
- Enter passphrase: Create passphrase
- Enter same passphrase again: Enter created passphrase
- Your identification has been saved as id_rsa
- Your public key has been saved as id_rsa.pub
- On webserver sudo vim /etc/ssh/sshd_config PasswordAuthentication yes
- sudo systemctl restart sshd
- ssh-copy-id username@192.168.1.2, you will be prompted (first time, once) for host:192.168.1.2 key fingerprint for known_hosts ,enter yes, then you will be prompted for password, then you will see number of key(s) added: 1
- Your id_rsa.pub (public key) has been copied in the webserver at ~/.ssh/authorized_keys
- Revert sudo vim /etc/ssh/sshd_config PasswordAuthentication no ,and, sudo systemctl restart sshd
- ssh username@192.168.1.2, prompt for password to unlock private key (passphrase), you get logged into webserver using passphrase only.
- exit (exit from webserver)
- mkdir ~/webterse_temp
- sudo apt-get install sshfs

Mount to webterse_temp on client machine: from username prompt

- sshfs username@DHCP-LAN-ip:/var/www/html ~/webterse_temp
- Prompt for password to unlock private key (passphrase), will not be asked, as you already logged in using ssh, password is remembered unless you poweroff client machine, but you will be logged into webserver using key based authentication only.

- cd webterse_temp
- ls
- cp index.html ~/Documents
- cd
- fusermount -u ~/webterse_temp

  You have been able to login using passphrase (private key) for both ssh and sshfs.

  For Windows-Laptop-PC, generate Private-Public Key using puttygen, type passphrase, save public key, save private key for example wd_rsa.pub and wd_rsa

- On webserver, backup authorized_keys (cp authorized_keys authorized_keys.bak) and append wd_rsa.pub to ~/.ssh/authorized_keys (cat wd_rsa.pub >> ~/.ssh/authorized_keys)
- sudo vim ~/.ssh/authorized_keys and make the appended wd_key format in one line beginning with ssh-rsa and ending in username@Windows-Laptop-PC (computer name)
- systemctl restart sshd
- In Putty, type 192.168.1.2 in Host Name, double-click SSH on left bottom, click Auth, on right in Private key file for authentication click Browse to select the private key wd_rsa, click Open and then click Open and enter passphrase to login to webserver.
- Now, you have logged in using Putty with key-based authentication from Windows Laptop into Ubuntu webserver.
- You can see the output of the shell/terminal during ssh-copy-id process and subsequent login (Ubuntu67VM and Putty) at github.com/gcgithub67/SSH-Copy-Id or Click here.

1.3.4 Certificate based authentication being your own CA

- SSL-TLS certificate signed by you (yourself) instead of real Certificate Authority (CA), for certificate based authentication on private-LAN/own-Email-server.
- Article for issueing own certificates can be found on arstechnica.com/information-technology/2014/04/taking-e-mail-back-part-4-the-finale-with-webmail-everything-after/4/ or Click here. We will be doing this in Section 2 i.e. email-server.
- Chrome can be downloaded and installed on ubuntu from google website and there is option of importing certificate in chrome web browser.

1.3.5 Installing DNS server BIND9, after taking static-ip and certbot

- You can read about Hairpinning/NAT loopback/Reflection versus own DNS Server (BIND9) for private LAN for accessing website through domain/subdomain in the web browser using the same Internet connection as that of your webserver.
- The DNS server in the tutorial mentioned below, will provide caching and name-resolution/ reverse-name-resolution in the internal/local DHCP LAN address range, not accessible externally from internet.
- You can read about How to setup a LAN DNS server using Bind9 on Ubuntu at cahilig.net/2008/07/how-setup-lan-dns-server-using-bind9-under-debian-etch-and-ubuntu-804 or Click here. In the tutorial, instead of main.debian.lan, for example main.webterse.com can be used with A record (192.168.1.2) and PTR (2) for main. There is a CNAME alias www record for main. You have to fill details using the format given in this tutorial, BIND9 will restructure (answer) the format automatically.
- Then create same A (192.168.1.2) and PTR (2) records for blog-coded and mail in the respective zone-files.

- In zone-files (forward and reverse), hostmaster.webterse.com in place of admin.debian.lan (email-webmaster@webterse.com which is written as webmaster.webterse.com in zone-files is already made at Godaddy domain manager, so I am using hostmaster.webterse.com instead).
- For Serial no. (starting with year 2019), type webterse.com in SOA at diggui.com
- In named.conf.options, type, listen-on port 53 { 127.0.0.1; 192.168.1.0/24; }; ,then forwarders section { 202.xx.xxx.xx (wired broadband isp dns); 8.8.8.8; 8.8.8.4; }, type, allow-query { 127.0.0.1; 192.168.1.0/24; }; ,then, allow-transfer { 127.0.0.1, 192.168.1.0/24; };, you do not need to enable recursion for home LAN.
- In named.conf.local, include "/etc/bind/rndc.key" and in zone-files, allow-update {key rndc-key; };
- /etc/init.d/bind9 reload, systemctl restart bind9, systemctl status bind9
- In client machine browser clear everything, in /etc/resolv.conf edit nameserver 192.168.1.2 ,Now, you can access www.webterse.com, webterse.com, blog-coded.webterse.com, mail.webterse.com and https://192.168.1.2 in browser, from client machine on LAN (another Windows laptop for example having LAN ip 192.168.1.3 on airtel broadband wifi/cable connected to the router) running Ubuntu desktop, for example ubuntu67vm (computer name) virtual machine (Virtual box) in bridged adapter installation.
- www.webterse.com, webterse.com, blog-coded.webterse.com, mail.webterse.com and https://192.168.1.2 can also be accessed from Windows laptop having DHCP LAN ip let's say 192.168.1.4
- Edit ,listen, in www virtual host file to be, listen 443 ssl default_server, as I have subdomains (to match correctly ip-address and LetsEncrypt certificate for domain (webterse.com, www.webterse.com) on typing https://192.168.1.2 in the browser), then /etc/init.d/nginx reload.
- Bind9 will resolve https://192.168.1.2 either to the domain or to anyone of the subdomains, depending upon the corresponding user-defined virtual host file nginx configuration for that domain/subdomain, as the domain (webterse.com, www.webterse.com) & the subdomains (2 in number: blog-coded.webterse.com, mail.webterse.com) have same DHCP LAN ip 192.168.1.2, that is, on the same Webserver. The actual virtual host files are, for webterse.com and www.webterse.com (www, user-defined, could have been a different name, let's say eg.wterse), for blog-coded.webterse.com (blog-code) and for mail.webterse.com (memail) respectively. Reverse translation is not distinct.
- www (in www.webterse.com) can be thought of as a subdomain of webterse.com
- In bridged adapter virtual box installation (Settings->Network->Adapter1->Attached to->Bridged Adapter), your ubuntuVM (running on Windows Laptop) will have DHCP Lan ip 192.168.1.3, 192.168.1.4 (or picked at random 192.168.1.x) will be the Windows laptop DHCP LAN ip and lets's say 192.168.1.6 will be the DHCP LAN ip of your Android smartphone. Also, you can assign 2GB RAM and 100 GB Hard Disk.
- In /etc/systemd/resolved.conf uncomment DNS, and type 192.168.1.2, and reboot to make the change persist.
- When you access Webserver using https://192.168.1.2 over LAN, the firefox/chrome browser shows a lock-with-an-exclaimation-mark-inside-a-triangle, if you click on this, it shows connection is not secure. This means that your certificate cannot be validated by the firefox/chrome browser over LAN for Let'sEncrypt to be a trusted CA, but your connection is still encrypted, as Lets's Encrypt gave certificate for domain/subdomain and not LAN ip address. Also, if you click Blog and login to WordPress (dashboard CMS), your connection switches to secure connection over internet. Also, Let'sEncrypt Authority X3 is present as one of the trusted CA's in the certificate manager of firefox/chrome.

- You should check for formatting-errors while creating zone files, named-checkconf /etc/bind/named.conf (the command will check for errors in both named.conf.local and named.conf.options). If on entering this command, the output is empty prompt line, then there are no errors.
- You can read about types of DNS server configuration in BIND9 manual at https://www.bind9.net/manuals or Click here.
- You can output your various DNS records using diggui.com on another laptop and at your own webserver terminal/shell using dig command.
- It is important to type-and-see that webterse.com, www.webterse.com, blog-coded.webterse.com and mail.webterse.com ,all, in [A] record should show your-static-ip at diggui.com or Click here.
- You can see my actual BIND9 forward-reverse-zone-files (format restructured-answered by BIND9 automatically), DHCPd.conf, named.conf.local, named.conf.options and GoDaddy DNS records at github.com/gcgithub67/BIND9-DHCP or Click here. On mobile-phone click at Desktop version bottom right to see files (images).

1.3.6 Installing isc-dhcp-server, after taking static-ip and certbot

- DHCP server is configured to make it work in tandem with BIND server.
- You can read about how to setup dhcp configuration /etc/dhcp/dhcpd.conf settings at blog.bigdinosaur.org/running-bind9-and-isc-dhcp/ or Click here.
- The dhcpd.conf file consists of statements which fall into two broad categories- parameters and declarations. Parameter statements either say how to do something (e.g. how long a lease to offer), whether to do something (e.g., should dhcpd provide addresses to unknown clients), or what parameters to provide to the client (e.g., use gateway 202.xxx.xxx.x). Declarations are used to describe the topology of the network, to describe clients on the network, to provide addresses that can be assigned to clients, or to apply a group of parameters to a group of declarations. You can read dhcp manual pages at kb.isc.org/docs/isc-dhcp-41-manual-pages-dhcpdconf#DESCRIPTION or Click here.
- Though the Airtel modem-cum-router has an option of fixing/making-static DHCP LAN ip addresses to MAC addresses, apart from static DHCP LAN ip addresses, isc-dhcp-server parameters and declarations are brought to use for overall management of LAN network.
- To install dhcp, sudo apt-get install isc-dhcp-server and in dhcpd.conf uncomment/type:
- include "/etc/bind/rndc.key"
- option domain-name "webterse.com";
- option domain-name-servers nsXX.webterse.com, nsXY.webterse.com;
- default-lease-time 1814400;
- max-lease-time 1814400;
- ddns-update-style interim;
- ddns-updates on;
- update-static-leases on;
- allow unknown-clients;
- use-host-decl-names on;
- authoritative;
- log-facility local7;
- zone webterse.com. { primary localhost; key rndc-key; }
- zone 1.168.192.in-addr-arpa. { primary localhost; key rndc-key; }
- subnet 192.168.1.0 netmask 255.255.255.0 { range 192.168.1.2 192.168.1.254; option subnet-mask 255.255.255.0; option routers 192.168.1.1; option domain-name-servers 192.168.1.2; option domain-name "webterse.com"; ddns-domainname "webterse.com"; ddns-rev-domainname "in-addr.arpa."; }

- host main.webterse.com { hardware ethernet d3:xx:xx:xx:xx:xx; fixed-address 192.168.1.2; ddns-hostname "main"; }
- systemctl restart isc-dhcp-server
- systemctl status isc-dhcp-server

DHCP will add (apart from ubuntu67vm [A] and [PTR] record) Windows-Laptop-PC(computer name) also, with TXT record for [A] record and corresponding [PTR] record. Same records will be added for your Android smartphone.

1.3.7 Generating and uploading sitemap for domain/subdomain

For Domain: On www.xml-sitemaps.com Enter webterse.com to generate and download sitemap.xml

- Copy sitemap.xml to /var/www/html
- Log into Google Search Console using Gmail id and password, Add Property webterse.com
- Google Search Console for verifying domain will ask you to authorize adding TXT record to GoDaddy DNS records. After authorizing, google search console will add your domain in the Property List.
- Refresh F5. You may have to Add Property again (due to just added TXT record propagation time), for verification to be successful.
- After successful verification, add sitemap url https://www.webterse.com/sitemap.xml
- Refresh F5

For Subdomain: On www.xml-sitemaps.com Enter blog-coded.webterse.com and download sitemap.xml

- Rename it to sitemapblog-coded.xml and copy to /var/www/htmln
- Log into Google Search Console using Gmail id and password, Add Property blog-coded.webterse.com
- Google Search Console will auto-add your subdomain in the Property List.
- Add sitemap url https://blog-coded.webterse.com/sitemap.xml
- Refresh F5

SEO: You can read about SEO (search engine optimization) and Responsive design (setting viewport). You can mouse-click-right and view page source code of index.html (home).

Responsive web design: Article on responsive web design templates can be found on w3schools.com/css/css_rwd _templates.asp or Click here.

- Microsoft Expression Web 4 editor can be used to test static web page template offline.

1.3.8 Miscellaneous

- HAProxy: Load Balancer etc. You can read on haproxy website.

1.3.9 For experimental purpose, webserver can be developed using Laptop having Ubuntu 18.04 LTS Desktop version or Laptop having Windows OS with VirtualBox running Ubuntu 18.04 LTS Desktop version. GitHub can be used as software/document version control repository.

1.3.10 node.js (built on Chrome's V8 JavaScript engine) for Webserver development on Windows/macOS/Linux came up during search and development on Internet.

1.3.11 GatsbyJS (based on React) for website and apps development came up during search and development on Internet. For migration, data can be pulled-in from WordPress CMS.

2. Email-Server: Installation on the same Webserver-Laptop, using IMAP only. We will also be doing Certificate based authentication for Roundcube LAN clients.

- On the same Webserver-Laptop, enable HTTPS subdomain mail.webterse.com for Email-Server, edit (from main to mail) in /etc/hosts 192.168.1.2 mail.webterse.com and in etc/hostname mail.webterse.com ,also, edit references (from main to mail) in zone-files, dhcpd.conf
- Edit in ,memail, virtual host file, listen 443 ssl default_server; (to match correctly ip-address and LetsEncrypt certificate for subdomain (mail.webterse.com) on typing https://192.168.1.2 in the browser) and in ,www, virtual host file, remove default_server from listen line, then /etc/init.d/nginx reload.
- There is a tutorial (using IMAP only) on How to run your own e-mail server with your own domain, arstechninca.com/information-tecnology/2014/02/how-to-run-your-own-e- mail-server-with-your-own-domain or Click here.
- In /etc/postfix/virtual (for outgoing from Roundcube to Gmail) line1 firstname@webterse.com firstname@webterse.com, (for incoming in Roundcube from Gmail) line2 firstname@mail.webterse.com firstname@webterse.com
- While sending from gmail, the sender is firstname@mail.webterse.com and while sending from roundcube the sender (logged into roundcube as firstname@webterse.com) is firstname@webterse.com
- In /etc/postfix/virtual-mailbox-domains type, webterse.com OK
- In /etc/bind/named.conf.options, in forwarders { 8.8.8.8; 8.8.4.4; }; (both are google dns)

For mail-stack-delivery, we will be installing from default Ubuntu repository:

- sudo apt-get update
- sudo apt-get install mail-stack-delivery ,during installation, select Internet Site, type (though default selected by system) in System mail name: mail.webterse.com

2.1 In the tutorial, the following has been configured:

- Postfix, to send and receive e-mail.
- Dovecot, for IMAP.
- SpamAssassin, Pyzor, Razor to keep spam out of your inbox.
- OpenDKIM

- ClamAV, to filter out viruses.
- Sieve, to set up mail filters and rules.
- Adding email user-account in MUA (mail user agent), for example Microsoft Outlook in Windows.

POP and IMAP Account Settings:: User Information:Your Name-Type fullname Email Address-firstname@webterse.com Server Information:Account Type-IMAP Incoming mail server-mail.webterse.com Outgoing mail server(SMTP)-mail.webterse.com Logon Information:User Name-firstname@webterse.com Password-type your password and lastly tick both the checkbox for Remember password as well as Require logon using Secure Password authentication (SPA). Click More Settings: General-Mail Account-firstname@webterse.com Outgoing Server-Log on using-User Name-firstname@webterse.com Password-type your password and tick both checkboxes for remember password as well as Require secure Password Authentication Advanced-Incoming server (IMAP) 993 SSL Outgoing server(SMTP) 587 TLS, click OK. Click Next, you will be prompted for installing Certificate (based authentication of section 2.2) and then Test Account Settings (Tasks: Log onto incoming mail server (IMAP) and Send test e-mail message) will be completed. I configured Outlook after section 2.3, that is after Certificate based authentication for Roundcube and Roundcube Webmail working successfully.

- Postscreen and IP tables for rate limiting.
- Roundcube for webmail (using web browser)
- MySQL, for Roundcube's database.
- Nginx and PHP-FPM, to serve out Roundcube over the Web.
- DKIM, SPF(TXT), MX records in domain manager of domain provider.
- Now, click on Email-server in menu to complete the configuration.

2.2 Certificate based authentication for Roundcube mail clients on LAN.

- X.509 is a standard defining the format of public key certificates.
- PKCS 12 defines an archive file format for storing many cryptography objects as a single file.

2.2.1 root key, CA certificate

- cd /etc/ssl/private
- openssl genrsa -des3 -out webterse.com.key 4096
- Enter and Verify passphrase enter eg. web#xx
- openssl req -new -x509 -days 3065 -key webterse.com.key -out webterse.com.crt
- Prompt for passphrase enter web#xx
- Series of Prompts for information Country IN, State UP, CITY Delhi, ORG NA, UNIT NA, Common Name mail.webterse.com, EMAIL hostmaster@webterse.com

firstname (root user) key, CSR

- openssl genrsa -des3 -out firsname.key 4096
- Enter & Verify passphrase enter eg. firstname#xx
- openssl req -new -key firstname.key -out firstname.csr
- Prompt for firstname.key passphrase enter firstname#xx
- Series of Prompts for information Country IN, State UP, CITY Delhi, ORG NA, UNIT NA, Common Name your_actual_name (fullname), EMAIL firstname@webterse.com, challenge password skip-enter, optional company name skip-enter

Sign firstname.csr with webterse.com.cert and webterse.com.key to produce self-signed personal certificate firstname.pem

- openssl x509 -CA webterse.com.crt -CAkey webterse.com.key -CAcreateserial -days 720 -req -in firstname.csr -out firstname.pem
- Prompt for webterse.com.key passphrase enter web#xx

Package self-signed certificate and key for installation on computers (or smartphone) to output firstname.pfx (pem packaged to pfx)

- openssl pkcs12 -export -out firstname.pfx -inkey firstname.key -in firstname.pem -certfile webterse.com.crt
- Prompt for firstname.key passphrase enter firstname#xx
- Enter and Verify export password enter eg. export#xx
- Copy firstname.pfx in Windows Laptop, mouse right click, select Install (import) PFX, Current User, Specify the file location, enter export#xx in Password, select automatically select the certificate store based on the type of certificate
- firstname.pfx appears in chrome->settings->advanced->manage-certificates->Personal list

2.2.2 client1 (user) key, CSR. The client1 can bring his own CSR to get it signed while keeping the key (private) to himself at his client desktop on LAN.

Create client1 on LAN: For testing of client1 certificate authentication (before you take PTR (reverse) record for mail.webterse.com with your wired broadband ISP). firsname, (root user) was already created before.

- doveadm pw -s SSHA512
- Enter and ReEnter passphrase eg. client1#xx
- Copy the encrypted string in /etc/dovecot/passwd.db for client1.
- Before you uncomment or type the lines for certificate based authentication in file ,memail, virtual host nginx file for mail.webterse.com, you can login to Roundcube with client1@webterse.com and password client1#xx
- After you uncomment or type lines for certificate based authentication in file ,memail, virtualhost nginx file for mail.webterse.com, you can login to Roundcube with client1.pfx installed (imported) in computer/browser (client1 authenticates himself to email-server), and client1@webterse.com and password client1#xx.

client1 (user) key, CSR

- cd /etc/ssl/private
- openssl genrsa -des3 -out client1.key 4096
- Enter & Verify passphrase enter eg. client1#xx
- openssl req -new -key client1.key -out client1.csr
- Prompt for client1.key passphrase enter client1#xx
- Series of Prompts for information Country IN, State Delhi, CITY Delhi, ORG NA, UNIT NA, Common Name your_actual_name (client1), EMAIL client1@webterse.com, challenge password skip-enter, optional company name skip-enter

Sign client1.csr with webterse.com.cert and webterse.com.key for client1, to produce signed client1 certificate client1.pem

- openssl x509 -CA webterse.com.crt -CAkey webterse.com.key -CAcreateserial -days 720 -req -in client1.csr -out client1.pem
- Prompt for webterse.com.key passphrase enter web#xx

Package client1 certificate and key for installation on computers (or smartphone) to output client1.pfx (pem packaged to pfx)

- openssl pkcs12 -export -out client1.pfx -inkey client1.key -in client1.pem -certfile webterse.com.crt
- Prompt for client1.key passphrase enter client1#xx
- Enter and Verify export password enter eg. exportc1#xx
- Copy client1.pfx in Windows Laptop, mouse right click, select Install (import) PFX, Current User, Specify the file location, enter exportc1#xx in Password, select automatically select the certificate store based on the type of certificate
- client1.pfx appears in chrome->settings->advanced->manage-certificates->Personal list

2.2.3 In memail file, nginx virtual host file for mail.webterse.com

- ssl_client_certificate /etc/ssl/private/webterse.com.crt
- ssl_trusted_certificate /etc/ssl/private/webterse.com.crt
- ssl_verify_client on; [Comment: Client verification]
- location / {
- if ($ssl_client_s_dn !~* "firstname@webterse.com| client1@webterse.com") { [Comment: Further matched and controlled Client list]
- return 301 http://www.jurassicsystems.com/;
- error_page 403 @fallback;
- }
- location @fallback {
- return 301 http://www.jurassicsystems.com/;
- }

Clear browser history, everything, with only a blank page opened in chrome, restart Computer.

Enter mail.webterse.com in browser, Select certificate at Prompt, Login Roundcube firstname@webterse.com password dove#xx

Enter mail.webterse.com in browser, Select certificate at Prompt, Login Roundcube client1@webterse.com password client1#xx

2.2.4 Type in shell (openssl has already been installed from ppa:ondrej), openssl s_client -connect mail.webterse.com:443, to check connection with certificate details for mail.webterse.com (LetsEncrypt as well as your own root CA certificate). Also, same connection with certificate details for 192.168.1.2:443 and (localhost) 127.0.0.1:443

2.2.5 If you install signed-certificate on Android smartphone, then you can Login to Roundcube webmail on home LAN using wired broadband ISP and on world-wide-web using Mobile internet.

- In mobile phone, settings->security->Install from SD card

2.3 Lastly, take only PTR (reverse) record for mail.webterse.com with broadband ISP Airtel.

- static IP address, resolve to—mail.webterse.com
- Airtel tech support calls it PTR update of domain. That is, now, [PTR] your-static-ip should output mail.webterse.com at diggui.com (initially it resolved to webterse.com).
- option domain-name and ddns-domainname in /etc/dhcp/dhcpd.conf gets automatically updated to mail.webterse.com (initially webterse.com)
- You can see Roundcube Login Inbox folder and Sent folder images at github.com/gcgithub67/RoundcubeDetails or Click here.

Copyright © webterse.com All Rights Reserved.

To the top

Powered by Nginx

office (000) 000-0000
fax (000) 000-0000
toll-free (000) 000-0000

Installing Repositories

- sudo /bin/bash
- sudo apt-get update
- sudo apt-get upgrade
- sudo apt-get install software-properties-common
- sudo apt-get update
- sudo apt-get install -y language-pack-en-base && export LC_ALL=en_US.UTF-8 && add-apt-repository -y ppa:ondrej/nginx && add-apt-repository -y ppa:ondrej/php
- sudo apt-get update

Installing Nginx and php-fpm

- sudo apt-get install nginx
- nginx 1.16.0 will be installed.
- sudo apt-get install php7.2-fpm
- PHP version 7.2.20-2 from php7.2-fpm will be installed.
- sudo apt-cache search php7.2-fpm gives list of all extensions/modules pulled-in during installation of php7.2-fpm.
- sudo apt-get install php7.2-mysql
- php7.2-mysql connector will be installed (connector can be installed afterwards also, that is, after installing mysql database server).
- Type reboot/poweroff

You can read arstechnica.com How to set up a safe and secure web server or Click here.

You can read arstechnica.com Web served, part 3: Bolting on PHP with PHP-FPM or Click here.

Some basic vim editor commands

- sudo vim /dir/file_name
- Escape->:wq write and quit (save and exit)
- Escape->:w only write to file (save changes with file being open)

- Escape->:qa! quit without saving file (any change to file, if you happen to open a wrong filename or wrong path to correct filename :qa! will not create that file)
- Escape->yy->p place the cursor where to yank yy->p (copy and paste line)
- Escape->v->d->p (After pressing v-> place the cursor and then select lines by pressing right arrow to cut d-> and paste at cursor location p

Configuring Nginx: virtual host file www

- cd /etc/nginx/sites/available
- cp default www
- www is the virtual host file, virtual host file configuration is also referred to as nginx configuration.
- sudo vim www
- Insert index.php in index index.html index.htm index.nginx-debian.html;
- server_name localhost (later webterse.com www.webterse.com during certbot execution)
- Add location / { try_files $uri $uri/ = 404; }
- Add location ~ \.php$, add try_files $uri = 404; , allow 192.168.1.0/24; , allow 127.0.0.1; uncomment include snippets/fastcgi-php.conf; , uncomment and make path as fastcgi_pass unix:/var/run/php/php5.6-fpm.sock;
- In above location (php), add fastcgi_param SCRIPT_FILENAME $document_root$fastcgi_script_name; and fastcgi_intercept_errors on;
- Add location ~ /\.ht , uncomment this location , uncomment deny all;
- Add location ~ /\. {access_log off; log_not_found off; deny all;}
- Add location ~ ~$ {access_log off; log_not_found off; deny all;}
- sudo ln -s /etc/nginx/sites-available/www /etc/nginx/sites-enabled/
- cd /etc/nginx/sites-enabled
- rm default
- Test and check for errors (example closing server {} brace), your www configuration by typing: sudo nginx -t
- sudo systemctl restart nginx or sudo /etc/init.d/nginx reload
- Type your IPaddress in browser you will get Welcome to nginx server webpage.

Configuring fastcgi_params

- In /etc/nginx sudo vim fastcgi_params
- Type at bottom fastcgi_buffer_size 128k; fastcgi_buffers 4 256k; fastcgi_busy_buffers_size 256k;

Configuring nginx.conf

- In /etc/nginx sudo vim nginx.conf edit pid /var/run/nginx.pid
- user www-data;
- worker_processes 4;
- server_tokens off;
- client_max_body_size 4096k;
- client_header_timeout 10;
- keepalive_timeout 10 10;
- send_timeout 10;
- gzip on;
- gzip_disable "msie6";
- gzip_min_length 1100;
- gzip_vary on;
- gzip_proxied any;
- gzip_buffers 16 8k;
- gzip_types text/plain text/css application/json application/x-javascript text/xml application/xml application/rss_xml text/javascript image/svg+xml applicatiom/x-font-ttf font/opentype application/vnd.ms-fontobject;

- After Gzip settings, add, ssl_session_cache shared:SSL:10m;

Testing Configuration of php-fpm(with nginx)

- cd /var/www/html
- sudo vim info.php
- Type a php-info script(search on internet).
- Type your IPaddress/info.php in browser.
- You will get php webpage which means you have set up php-fpm processing with Nginx successfully.

Putting your own website developed in the editor Expression Web 4

- Install Microsoft Expression Web 4
- Open Expression Web 4, click Site in the menubar and select New Site, select Templates, select Small Business 1, save it in a new folder mysite.
- Go to the new folder mysite, open master.dwt template and all default.html in the editor , make changes to your liking as per your own website pages, content.
- Save the changes across all files for any change in any of the default.html, style1.css or master.dwt file.
- Copy all contents of folder mysite on pendrive.
- Insert pendrive on Ubuntu Server 18.04.2 LTS laptop.
- Press Enter.
- sudo fdisk -l
- mkdir /media/pdrive
- sudo mount -t vfat /dev/sdb1 /media/pdrive
- cd /var/www/html
- cp index.nginx-debian.html index.nginx-debian.htmlSave
- rm index.nginx-debian.html
- cp -avr /media/pdrive/mysite/. /var/www/html
- sudo umount /media/pdrive
- Type your IPaddress in browser, you will get webpage of your own website.

apcu, memcache: Nginx and php-fpm configuration

- sudo apt-get install memcached php-memcache
- In /etc/memcached.conf
  - Comment # -p 11211
  - Comment # -l 127.0.0.1
  - Type at bottom -s /tmp/memcached.sock
  - Type at bottom -a 666
- sudo apt-get install memcached php-apcu
  - In /etc/php/7.2/fpm/conf.d sudo vim 20-apcu
  - Type apc.shm_size = 128
  - sudo systemctl restart php7.2-fpm

php.ini configuration

- In /etc/php/7.2/fpm sudo vim php.ini and edit post_max_size = 2M and type-under-session session.save_handler = memcache session.save_path = unix:/tmp/memcached.sock
- mysql.default_socket = /var/run/mysqld/mysqld.sock
- sudo systemctl restart php7.2-fpm

php.conf configuration

- In /etc/php/7.2/fpm sudo vim php-fpm.conf and edit pid = /var/run/php/php7.2-fpm.pid

- Search on arstechnica.com web served, part 3: bolting on PHP with php-fpm for remaining php.conf settings.

www.conf configuration

- In /etc/php/7.2/fpm/pool.d sudo vim www.conf edit listen = /var/run/php/php7.2-fpm.sock
- Un-comment listen.owner = www-data;
- Un-comment listen.group = www-data;
- pm = dynamic
- pm.max_children = 10
- pm.start_servers = 4
- pm.min_spare_servers = 2
- pm.max_spare_servers = 6

my.cnf configuration

- In /etc/mysql/mysql.conf.d/mysqld.cnf type skip-networking at bottom.
- systemctl restart mysql

Home | Nginx-PHPfpm | MySql | Wordpress | Blog | Blog-coded MakingHTTPS | Email-Server | Site Map

Copyright © 0000 Company Name. All Rights Reserved.

office (000) 000-0000
fax (000) 000-0000
toll-free (000) 000-0000

Installing downloaded MySQL website Community Downloads (DEB-Bundle mysql-server_5.7.27-1ubuntu18.04_amd64.deb-bundle.tar) in order as given:

- In /usr/local mkdir mysql
- Place mysql-server_5.7.27-1ubuntu18.04_amd64.deb-bundle.tar in /usr/local/mysql
- tar -xvf mysql-server_5.7.27-1ubuntu18.04_amd64.deb-bundle.tar
- tar will result in 5 packages: mysql-common, community-client, client, community-server and server)
- sudo dpkg -i mysql-common
- sudo dpkg -i mysql-community-client
- sudo apt-get install -f (for missing lib)
- sudo dpkg -i mysql-community-client (after installing missing libaio1)
- sudo dpkg -i mysql-client
- sudo dpkg -i mysql-community-server
- sudo apt-get install -f (for missing lib)
    - Terminal will ask overwrite my.cnf Y(yes) with password (if previous mysql/mariadb database already installed, apart from php7.2-mysql connector). Choose overwrite Y(yes). Prompt (graphical page) to set root password follows.
    - If you have not already installed any previous mysql/mariadb database, apart from php7.2-mysql connector before, Prompt (graphical page) to set root password follows.
- sudo dpkg -i mysql-community-server (after installing missing libmecab2)
- sudo dpkg -i mysql-server
- Type in shell, mysql -u root -p and enter password. Type exit to come out of mysql prompt.
- It is IMPORTANT that graphical page prompt to set password appears.
- To install mysql_config --include: sudo apt-get install libmysqlclient-dev
- Type in shell, mysql_config
- After installing libmysqlclient-dev, your (-I:header) path is /usr/include/mysql
- After installation, your (-L:library) path is /usr/lib/x86_64-linux-gnu

my.cnf and mysqld.cnf settings

- In /etc/mysql my.cnf appears after and if only php7.2-mysql connector is installed on ubuntu server
- In /etc/mysql/mysql.conf.d mysqld.cnf appears after mysql-server_5.7.27-1ubuntu18.04_amd64.deb-bundle is installed on ubuntu server.
- For instance, if you have installed myql database server (and have not installed php7.2-mysql connector yet), then both my.cnf and mysqld.cnf will appear.

In case Prompt (graphical page) to set root password does not appear

- This means that you have installed/reinstalled/experimented-during-developemnt previous mysql/mariadb installations, which are interferring.
- You will have to clean previous mysql/mariadb database from your ubuntu server.
- sudo apt-get purge --auto-remove mariadb-server
- sudo apt-get purge --auto-remove mysql
- sudo apt-get purge --auto-remove mysql*
- sudo apt-get purge --auto remove php-mysql
- In /etc rm -r mysql
- In /lib rm -r mysql
- In /usr/sbin rm mysqld
- In /usr/sbin rm mysqld-debug
- reboot
- sudo systemctl restart php7.2-fpm
- reboot
- In /usr/sbin Check if mysqld and mysqld-debug reappear, if not remove and reinstall php7.2-fpm
- sudo apt-get install php7.2-mysql
- sudo systemctl restart php7.2-fpm
- Installing downloaded MySQL (DEB-Bundle) in order as given above.

Though I have not installed it, the latest (next after 5.7.27) is DEB Bundle: mysql- server_8.0.17-1ubuntu18.04_amd64.deb-bundle.tar

Home | Nginx-PHPfpm | MySql | Wordpress | Blog | Blog-coded | MakingHTTPS | Email-Server | Site Map

Copyright © 0000 Company Name. All Rights Reserved.

office (000) 000-0000
fax (000) 000-0000
toll-free (000) 000-0000

Creating WordPress Database

- sudo /bin/bash
- sudo mysql -u root -p
- Enter mysql_root_password
- create database wordpressdb character set utf8mb4 collate utf8mb4_unicode_ci;
- create user 'wproot'@'localhost' identified by 'mysql_root_password'; (keep password same for simplicity, though it can be different)
- grant all on wordpressdb.* to 'wproot'@'localhost' with grant option;
- flush privileges;
- show databases;
- exit

Downloading WordPress

- cd /var/www/html
- wget https://wordpress.org/latest.zip
- unzip latest.zip
- mv /var/www/html/wordpress /var/www/html/blog
- chown -R www-data:www-data /var/www/html/blog

Installing any Location (mkdir folder)

- For any created folder (under /var/www/html) for example, mkdir blog in /var/www/html, it is important to give it ownership rights. Type chown -R www-data:www-data /var/www/html/blog
- For any created folder (under /var/www), it is important to give it ownership rights. /var/www/html has ownership rights for user www-data by default.
- For the first-website on domain virtual host file, www, server_name localhost; (later changed to server_name webterse.com www.webterse.com; during certbot execution) and respective document root folder /var/www/html
- For another second-website on subdomain (more than one) virtual host file, blog-code, server_name blog-coded.webterse.com and respective document root folder /var/www/htmln, type chown -r www-data:www-data /var/www/htmln

Virtual host files (3 in total) are available on github at github.com/gcgithub67/virtual-host-files or Click here.

    - www [webterse.com] [www.webterse.com] (/etc/nginx/sites-available/www)
    - blog-code [blog-coded.webterse.com] (/etc/nginx/sites-available/blog-code)
    - memail [mail.webterse.com](/etc/nginx/sites-available/memail)
- On mobile phones, click on bottom right for desktop version, to see the files.

blog-code virtual host file configuration nginx

- location /blog/ {
- try_files $uri $uri/ /blog/index.php?$args;
- allow 192.168.1.0/24;
- allow 127.0.0.1;
- }
- location ~ /blog/.*\.php$ {
- allow 192.168.1.0/24;
- allow 127.0.0.1;
- try_files $uri = 404;
- include fastcgi_params;
- include snippets/fastcgi-php.conf;
- fastcgi_pass unix:/var/run/php/php7.2-fpm.sock;
- fastcgi_param SCRIPT_FILENAME $document_root$fastcgi_script_name;
- fastcgi_intercept_errors on;
- }

sudo ln -s /etc/nginx/sites-available/blog-code /etc/nginx/sites-enabled

Installing WordPress

- https://webterse.com/blog/wp-admin/install.php (Before taking static-ip and enabling HTTPS, local-ip or private-ip/blog/wp-admin/install.php)
- Database Name wordpressdb
- User Name wproot
- Database Host localhost
- Password mysql_root_password
- Table Prefix wordpressdb_
- Click Submit
- Site Title MyBlog
- Username mybloguser
- Password copy the generated password/type your password in place of generated password
- Your E-mail your gmail id
- allow search engines to index this site
- Click Install Wordpress
- Login to WordPress to Dashboard page of the CMS (Content Management System), to publish blog/website.

Re-Installing WordPress

- Delete wp-config.php in /var/www/html/blog
- Re-install as given above.

The instance of WordPress (Blog in the menu of the webterse.com website) is linked to webterse.com, but it can be a

seperate instance (on domain or subdomain) which can be used to make full-blown commercial website rather than just a blog.

Copyright © 0000 Company Name. All Rights Reserved.

MyWpBlog

Webterse Blog

Nginx-PHPfpm-MySQL

Welcome to Webterse Blog using WordPress. Click topic to discuss.

September 8, 2019 / 2 Comments

MyWpBlog / Proudly powered by WordPress

office (000) 000-0000
fax (000) 000-0000
toll-free (000) 000-0000

There is a tutorial on how to develop a blog using PHP and HTML code using tutorial at ilovephp.jondh.me.uk/en/tutorial/make-your-own-blog or Click here.

- Over some years, the tutorial has shaped out of six versions. The tutorial uses netbeans diff for code walkthrough.
- For Version 1, till section 6, that is, Adding a login system, the compiled source code can be found on github.com/gcgithub67/blog-coded or Click here.
- On mobile phone, click Desktop version, bottom-right, on Github page to see source-code files.
- For Version 1, full, All 12 sections, the compiled source code can be found on github.com/gcgithub67/blog-coded-full or Click here. Create .htaccess text file in the folder containing index.php and paste the following contents without bullets:
    - RewriteEngine on
    - RewriteCond %{REQUEST_URI} ^/(data|lib|templates|vendor)/
    - RewriteRule ^ - [L,R=404]
- In www virtual host file in /etc/nginx/sites-available/www, above server_name, we have list as: index index.html index.htm index.nginx-debian.html index.php;
- When you click Blog-coded in menu on website, default.html page opens (as index.html is before index.php in the list), although index.php is also present in blog-coded folder /var/www/html/blog-coded
- If you click Blog-coded in menu on website, then type index.php in place of default.html and press enter, the coded blog will be accessed as domain, webterse.com/blog-coded/index.php.
- So, if default.html (that is this page) is not present and index.php is present in blog-coded folder /var/www/html/blog-coded, then the coded blog can be accessed by clicking on Blog-coded in menu of the website.
- Alternatively, the coded blog can also be accessed as subdomain, blog-coded.webterse.com (to have a look-and-feel of it).
- Also, at www.taniarascia.com, under Articles, simple PHP applications are listed, for example, Create a Simple CRUD Database App: Connecting to MySQL with PHP (Part1: Create, Read) or Click here and Part2: Update, Delete)or Click here. The example uses PDO for MySQL (PHP Data Objects) as driver for MySQL database.
- With mysqli (i:improved) driver, you can only connect to MySQL database, but using PDO, you can connect to any database.

It can be Compiled and debugged using Netbeans, XAMPP (Apache, MySQL and PHPMyAdmin) in Windows/Ubuntu Desktop

version Operating System

- Install XAMPP, start Apache (webserver), start MySQL (MySQL password is blank).
- Place the source code folder in C:/xampp/htdocs
- In Netbeans IDE 8.2, Click on New Project: PHP Application from existing Sources
- Run configuration: Local website (running on local webserver).
- Browser: IDE's default web Browser (Project Properties)
- Run install.php (mouse-click-right on install.php file in Netbeans IDE) during development.
- After compiling, Install (webterse.com/blog-coded/install.php or blog-coded.webterse.com/install.php) on domain or subdomain respectively, over internet using web browser.

Or, there is option of Netbeans IDE 8.2 Internal web server for compiling and debugging

Adding A Record for subdomain blog-coded.webterse.com in GoDaddy DNS Record (Check your DNS provider FAQs for adding subdomain)

- [A] [blog-coded] [your-static-ip] [600seconds]

Home | Nginx-PHPfpm | MySql | Wordpress | Blog | Blog-coded | MakingHTTPS | Email-Server | Site Map

Copyright © 0000 Company Name. All Rights Reserved.

office (000) 000-0000
fax (000) 000-0000
toll-free (000) 000-0000

SSL/TLS Certbot Let'sEncrypt

- Point A record of Godaddy DNS to your-static-ip. There is propagation time before you can access your website using domain/subdomain.
- For Domain: webterse.com
- sudo apt-get update
- sudo add-apt-repository ppa:certbot/certbot
- sudo apt-get update
- server_name webterse.com www.webterse.com in /var/www/html for www virtual host file.
- sudo apt-get install certbot python-certbot-nginx
- sudo certbot --nginx -d webterse.com -d www.webterse.com
- website can be accessed as webterse.com or www.webterse.com
- Choose option 2: Redirect
- For Subdomain:blog-coded.webterse.com
- Add [A] [blog-coded] [your-static-ip] [600 seconds]
- sudo certbot --nginx -d blog-coded.webterse.com
- server_name blog-coded.webterse.com in /var/www/htmln for blog-code virtual host file.
- Choose option 2: Redirect
- website can be accessed as blog-coded.webterse.com
- Generally, subdomain is accessed as blog-coded.webterse.com and not as www.blog-coded.webterse.com
- [A] record is sufficient for certbot execution and for accessing subdomain.

Copyright © 0000 Company Name. All Rights Reserved.

office (000) 000-0000
fax (000) 000-0000
toll-free (000) 000-0000

Making domain (subdomain) available, that is HTTPS enabled mail.webterse.com for installing email-server

Adding DNS records for mail.webterse.com

- Only adding A record is sufficient for certbot certificate installation and accessing subdomain.
- [A] [mail] [your-static-ip] [1 Hour]

Enabling HTTPS

- mkdir /var/www/htmlm
- Copy default index.nginx-debian.html into /var/www/htmlm
- chown -R www-data:www-data /var/www/htmlm
- In /etc/nginx/sites-available cp default memail (you can use an existing virtual host file having configuration for location php, uncomment listen 80;, remove all certbot managed lines).
- server_name mail.webterse.com;
- sudo ln -s /etc/nginx/sites-available/memail /etc/nginx/sites-enabled
- sudo /etc/init.d/nginx reload
- Run sudo certbot --nginx -d mail.webterse.com and Choose option 2 for Redirect.
- The default page can be found on mail.webterse.com or Click here.
- If on entering mail.webterse.com in the browser, the default page says 400 bad Request no required SSL certificate was sent nginx, then you need a signed-certificate.pfx from the webterse.com webmaster to Login to Roundcube webmail on world-wide-web (as certificate based authentication has been configured of nginx virtual host file memail).

Configuration settings specific to my setup, rest TALLY & EDIT/ADD as given in the tutorial.

1. POSTFIX: In /etc/postfix/main.cf

- myhostname = mail.webterse.com
- mydestination = localhost, mail.webterse.com,localhost.webterse.com
- smtpd_tls_cert_file = /etc/letsencrypt/live/mail.webterse.com/fullchain.pem ,
- smtpd_tls_key_file = /etc/letsencrypt/live/mail.webterse.com/privkey.pem
- smtpd_tls_CAfile = /etc/ssl/certs/ca-certificates.crt
- mynetworks = 127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128 192.168.1.0/24

2. POSTFIX: In /etc/postfix/master.cf

- Same as tutorial

3. /etc/aliases

- postmaster: hostmaster@webterse.com
- root: hostmaster@webterse.com
- www-data: hostmaster@webterse.com
- type in shell newaliases.
- webmaster@webterse.com has already been made at Godaddy domain manager.

4. /etc/postfix/canonical

- www-data@www.webterse.com postasurus@webterse.com
- type in shell postmap /etc/postfix/canonical

5. /etc/postfix/virtual-mailbox-domains

- webterse.com OK
- type in shell postmap /etc/postfix/virtual-mailbox-domains

6. /etc/postfix/virtual-mailbox-users

- firstname@webterse.com firstname@webterse.com
- postbot@webterse.com postbot@webterse.com
- hostmaster@webterse.com hostmaster@webterse.com
- type in shell postmap /etc/postfix/virtual-mailbox-users
- You will be able to recieve emails from webmaster@webterse.com (Godaddy) but not be able to send email to webmaster@webterse.com (Godaddy)

7. /etc/postfix/virtual

- firstname@webterse.com firstname@webterse.com
- firstname@mail.webterse.com firstname@webterse.com
- hostmaster@webterse.com hostmaster@webterse.com
- hostmaster@mail.webterse.com hostmaster@webterse.com
- postbot@webterse.com postbot@webterse.com
- postmaster@webterse.com hostmaster@webterse.com
- root@mail.webterse.com hostmaster@webterse.com
- root@webterse.com hostmaster@webterse.com
- abuse@webterse.com hostmaster@webterse.com
- type in shell postmap /etc/postfix/virtual
- service postfix restart
- You can send to gmail using firstname@webterse.com, hostmaster@webterse.com And receive from gmail using firstname@mail.webterse.com, hostmaster@mail.webterse.com respectively.

8. A home for your virtual users' mail

- There's already a directory on the server, /var/mail/
- The first time a virtual user receives mail, Dovecot will automatically create everything the virtual user needs under /var/mail/vmail/*.
- groupadd -g 5000 vmail
- useradd -g vmail -u 5000 vmail -d /var/mail/vmail -m

9. Dovecot MDA: /etc/dovecot/conf.d/10-ssl.conf

- Comment '#' ssl_cert and ssl_key

10.Dovecot MDA: /etc/dovecot/conf.d/99-mail-stack-delivery.conf

- protocols = imap sieve
- ssl = yes
- Append less-than sign before /etc in ssl_cert and ssl_key lines as in tutorial.
- ssl_cert = /etc/letsencrypt/live/mail.webterse.com/fullchain.pem
- ssl_key = /etc/letsencrypt/live/mail.webterse.com/privkey.pem

- ssl_client_ca_dir = /etc/ssl/certs (Dovecot isn't running in a chroot jail, and you can give it the path to /etc/ssl/certs rather than needing to use a single root CA file.)
- (Copy from /etc/letsencrypt/options-ssl-nginx.conf) ssl_cipher_list = ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA256:ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES256-SHA384:ECDHE-RSA-AES128-SHA:ECDHE-ECDSA-AES256-SHA384:ECDHE-ECDSA-AES256-SHA:ECDHE-RSA-AES256-SHA:DHE-RSA-AES128-SHA256:DHE-RSA-AES128-SHA:DHE-RSA-AES256-SHA256:DHE-RSA-AES256-SHA:ECDHE-ECDSA-DES-CBC3-SHA:ECDHE-RSA-DES-CBC3-SHA:EDH-RSA-DES-CBC3-SHA:AES128-GCM-SHA256:AES256-GCM-SHA384:AES128-SHA256:AES256-SHA256:AES128-SHA:AES256-SHA:DES-CBC3-SHA:!DSS
- mail_home = /var/mail/vmail/%d/%n
- mail_location = maildir:/var/mail/vmail/%d/%n/mail:LAYOUT=fs
- auth_username_chars = abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ01234567890.

11. /etc/dovecot/conf.d/10-mail.conf

- Comment '#' mail_location = mbox:~/mail:INBOX=/var/mail/%u

12. /etc/dovecot/conf.d/10-auth.conf

- Comment '#' auth_mechanisms = plain

13. /etc/dovecot/conf.d/auth-system.conf.ext

- Edit auth-system.conf.ext and comment out every uncommented line in the passdb stanza, including its start and end lines
- Edit auth-system.conf.ext and comment out every uncommented line in the userdb stanza, including its start and end lines

14. /etc/dovecot/passwd.db

- Passwords for firstname@webterse.com postbot@webterse.com hostmaster@webterse.com

15. /etc/dovecot/conf.d/15-mailboxes.conf

- As in tutorial
- service dovecot restart
- doveccot -n

16. OpenDKIM

- sudo apt-get install opendkim opendkim-tools
- service opendkim restart
- Same as in tutorial

17. Spamassassin

sudo apt-get install spamass-milter pyzor razor libmail-dkim-perl

OPTIONS="-x --max-children 5 --helper-home-dir /var/lib/spamassassin -u spamd -g spamd --siteconfigpath /etc/spamassassin --socketpath=/var/spool/postfix/spamassassin/spamd.sock --socketowner=spamd --socketgroup=spamd --socketmode=0660"

- spamassassin --lint
- sa-update

service spamassassin restart && service spamass-milter restart

17. Razor

- Same as in tutorial

18. Pyzor

- Same as in tutorial
- pyzor --homedir /var/lib/spamassassin/.pyzor discover
- CRITICAL Unknown command: discover
- PYZOR cat spam.test | spamassassin -D 2>&1|grep pyzor

19. CLAMAV

- (Skip this as zoo, lha has no installation candidate) sudo apt-get install clamav-milter arj bzip2 cabextract cpio file gzip lha lzop nomarch p7zip pax rar rpm unrar unzip zip zoo
- (Added lhasa jlha-utils) sudo apt-get install clamav-milter arj bzip2 cabextract cpio file gzip lha lzop nomarch p7zip pax rar rpm unrar unzip zip lhasa jlha-utils
- In new version, SOCKET_RWGROUP=postfix is configured in /etc/clamav/clamav-milter.conf as MilterSocketGroup postfix
- service clamav-daemon restart && service clamav-milter restart
- type in shell freshclam
- sudo lsof | grep freshclam
- sudo kill -9 pid (pid is second column number after you type sudo lsof | grep freshclam)
- freshclam
- sudo lsof /var/log/clamav/freshclam.log

20.Telling Postfix about your milters, /etc/postfix/main.cf

- milter_default_action = accept
- milter_connect_macros = j {daemon_name} v {if_name} _
- non_smtpd_milters = $smtpd_milters
- smtpd_milters = unix:/spamass/spamass.sock unix:/clamav/clamav-milter.ctl unix:/opendkim/opendkim.sock
- service postfix reload

21. MX record Godaddy

- [MX] [@] [mail.webterse.com (Priority: 20)] [1 Hour]

22. SPF (TXT) record Godaddy

- [TXT] [@] ["v=spf1 mx a ?all"] [1 Hour]

23. DKIM (TXT) record Godaddy

- (Copy string from /etc/opendkim/mail.txt) [TXT] [mail._domainkey] ["v=DKIM1; h=sha256; k=rsa; s=email;
"
"p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA2E5+UseaIVw3LzHHgxoTSXKC8chl7xDIp/
a5o1ZNM8O1BHuR/bOLSpB023IYyoG8lbWkgFAUKplSvYRpQ/21eg6pun3Ad+5i6hxiX2987lLjaJfN9cl
LLgBe2RbMp5XB0OcaS/S2+SxlHgFY2T6kI1vO76gr7qqW6hrJn901PpUBf+Eajez1z37OCMLeWmq/
yA2DAQvpW+YDzh"
"Dk060G1NkUK0HJKFc4qseHpuozxs1prQ9pCANNMZrUKx9OW2bUNod9F+MJaxEPSN4f
dlrKnTQkl6Fn383lCgWTcmehzMXyDB4wA3+y6nfjzXLklo0fQHqNp5wt0OLbmqCuIt26vQIDAQAB"] [1
Day]

24. PTR (reverse) record with wired broadband ISP Airtel

- static IP address, resolve to—mail.webterse.com

25. Sieve: E-mail filtering for spam fighting

- Example: sudo sieve-test envelopetest.sieve /var/mail/vmail/ bigdinosaur.org/lee/mail/cur/(message) -t - -Tlevel=matching
- sievec command on it to transform it into a binary .svbin file
- sievec yourrulefile.sieve

- If you do this as root, make sure to then chown the resulting .svbin file to vmail:vmail

26. Adding email-user in MUA Microsoft Outlook

- Same as tutorial

27. Postscreen and additional filtering

- (/etc/postfix/master.cf)#smtp inet n - y - - smtpd
- smtp inet n - - - 1 postscreen
- smtpd pass - - - - - smtpd
- dnsblog unix - - - - 0 dnsblog
- tlsproxy unix - - - - 0 tlsproxy
- submission inet n - - - - smtpd
- dovecot unix - n n - - pipe
- flags=DRhu user=vmail:vmail argv=/usr/lib/dovecot/deliver -f ${sender} -d ${recipient}
- (/etc/postfix/main.cf)postscreen_greet_action = enforce
- postscreen_dnsbl_action = enforce
- postscreen_access_list = permit_mynetworks
- postscreen_dnsbl_sites = zen.spamhaus.org, b.barracudacentral.org,bl.spamcop.net

28. rate limiting with iptables

- sudo apt-get install iptables-persistent
- /etc/iptables/rules.v4 (as given in tutorial)
- Be sure to modify "192.168.0.0/24" to point to your LAN subnet
- iptables-restore rules.v4
- iptables -L

29. Webmail (Roundcube): Nginx PHP-fpm

- Use http2 in place of spdy (deprecated) in domain (www) virtual host file i.e. listen 443 ssl http2; ,this, will be applied across subdomains automatically, check http2 enabling at tools.keycdn.com/http2-test
- location ~ ^/(README|INSTALL|LICENSE|CHANGELOG|UPGRADING)$ {deny all;}
- location ~ ^/(config|bin|SQL|logs|temp)/ { deny all;}

30. Webmail (Roundcube): MySQL

- sudo mysql -u root -p
- Enter mysql_root_password
- create database roundcubedb character set utf8mb4 collate utf8mb4_unicode_ci;
- create user 'rcroot'@'localhost' identified by 'mysql_root_password'; (keep password same for simplicity, though it can be different)
- grant all on roundecubedb.* to 'rcroot'@'localhost' with grant option;
- flush privileges;

31. Webmail: Roundcube

- Download Roundcube from Roundcube website:roundcubemail-1.3.10-complete.tar.gz
- Copy roundcubemail-1.3.10-complete.tar.gz to /var/www/htmlm
- tar zxfv roundcubemail-1.3.10-complete.tar.gz
- mv roundcubemail-1.3.10-complete roundcube
- cp -r roundcube/. /var/www/htmlm
- chown -R www-data:www-data /var/www/htmlm
- Then, type in web browser at mail.yourdomain.com/installer
- Roundcube Webmail Installer: 1. In section 1 check environment Install php7.2-xml Refresh, Install php7.2-xml Refresh, Install php7.2-intl Refresh, Install php7.2-ldap Refresh, Install php7.2-gd Refresh, Install php7.2-imagick Rfresh, systemctl restart php7.2-fpm, In /etc/php/7.2/fpm/pho.ini date.timezone Asia/Kolkata
- Roundcube Webmail Installer: 2. In section 2, type mysql_root_password and create config (as per tutorial, copy paste generated config into /var/www/htmlm/config/config.inc.php).

- Roundcube Webmail Installer: 3. In section 3, test config, Test IMAP (port 143, localhost) config: Username: firstname@webterse.com password: as you set in dovecot password, IMAP connect: OK (SORT capability: yes) and Test SMTP (port 25, localhost) send OK (type firstname@webterse.com in Sender and gmail-id in Recipient)
- You can see Roundcube configuration dettails at github.com/gcgithub67/RoundcubeDetails or Click here.

Home | Nginx-PHPfpm | MySql | Wordpress | Blog | Blog-coded | MakingHTTPS | Email-Server | Site Map

Copyright © 0000 Company Name. All Rights Reserved.