Apache, MySQL Checklist

Distribution Differences

- /etc/httpd/conf/httpd.conf (RHEL/CentOS/Fedora/Arch)
- /etc/apache/apache2.conf (debian/Ubuntu)

Basics

- Default root directory
    - /var/www/html or /var/www
- Test Config File Settings and syntax
    - httpd –t
- Access Log Files of Web Server
    - /var/log/httpd/access_log
    - /var/log/httpd/ssl_access_log
- Error Log files of Web Server
    - /var/log/httpd/error_log

1. Run Apache as separate User and Group

- Create Apache user and group
    - Groupadd apache-web
    - Useradd –d /var/www/ -g apache-web –s /bin/nologin apache-web
- Run Apache with created user
    - Nano /etc/httpd/conf/httpd.conf (RHEL/CentOS/Fedora/Arch)

      nano /etc/apache/apache2.conf (Debian/Ubuntu)
    - Look for “User” and “Group” and modify it as:
        - User apache-web
        - Group apache-web

2. Configuration Changes

Nano /etc/httpd/conf/httpd.conf (RHEL/CentOS/Fedora)

Nano /etc/apache/apache2.conf (Debian/Ubuntu)

Check folder structure first. All varibles/configurations may not be in the apache config

- Hide Apache Version and OS Identity
- How to find ServerTokens variable configuration
  - grep -ri 'ServerTokens' *
    - ServerSignature Off
    - ServerTokens Prod
- Disable Directory Listing
  - <Directory /var/www/html>
  - Options –Indexes
  - </Directory>

- Use Allow and Deny to Restrict access to Directories
  - <Directory />
  - Options None
  - Order deny,allow
  - Deny from all
  - </Directory>

- Disable Apache's following of Symbolic Links
  - Options –FollowSymLinks
- Turn Off Server Side Includes and CGI Execution
  - Options –Includes
  - Options –ExecCGI
- Enable Apache Logging
  - LogLevel warn
    - ErrorLog /var/log/httpd/example.com_error_log
    - CustomLog /var/log/httpd/example.com_access_log combined

- Disable the following modules by commenting with a #
  - Mod_imap
  - Mod_include
  - Mod_info

    - Mod_userdir
    - Mod_autoindex
- Save Configuration and restart service
    - Service httpd restart or service apache2 restart

3. Install Mod_Security

- On Ubuntu/Debian
    - Sudo apt-get install libapache2-modsecurity
    - Sudo a2enmod mod-security
    - Sudo /etc/init.d/apache2 force-reload
- On RHEL/CentOS/Fedora
    - Yum install mod_security
    - /etc/init.d/httpd restart

4. Generating SSL Certificates

- Generate SSL Keys
    - Openssl genrsa –des3 –out /etc/pki/tls/certs/example.com.key 1024
    - Openssl req –new –key /etc/pki/tls/certs/example.com.key –out /etc/pki/tls/certs/example.csr
    - Openssl x509 –req –days 365 –in /etc/pki/tls/certs/example.csr –signkey /etc/pki/tls/certs/example.com.key –out /etc/pki/tls/certs/example.crt
- Modify Apache Config again and add SSL Key
    - <VirtualHost 172.16.25.125:443>
    - SSLEngine on
    - SSLCertificateFile /etc/pki/tls/certs/example.com.crt
    - SSLCertificateKeyFile /etc/pki/tls/certs/example.com.key
    - --Only need for official cert---SSLCertificateChainFile /etc/pki/tls/certs/sf_budle.crt
    - ServerAdmin blah.blah@example.com
    - ServerName example.com

- DocumentRoot /var/www/html/example/
- ErrorLog /var/log/httpd/example.com-error_log
- LogL
- CustomLog /var/log/httpd/example.com-access_log common
- </VirtualHost>

Mysql

mysql -u -p

Create user 'groot' identified by 'gr00tzp@s$w0rd!;

grant select, insert, update on *.* to 'groot';