Apache/Nginx/Varnish

Apache vhost

```
vim /etc/httpd/conf/httpd.conf
```

> add (include vhosts/*.conf) at the bottom

```
mkdir /etc/httpd/vhosts
```

```
vim /etc/httpd/vhosts/domains.conf
```

```
#######################
###      NO SSL     ###
#######################
<VirtualHost *:80>
    DocumentRoot "/var/www/vhost/domain.com/"
    ServerName domain.com
    ServerAlias www.domain.com
   <Directory /var/www/vhost/domain.com/>
        Options Indexes FollowSymLinks MultiViews
        AllowOverride All
   </Directory>
   <Directory "/var/www/vhost/domain.com/must_mysql">
        AuthType Basic
        AuthName "Restricted Content"
        AuthUserFile /etc/httpd/.htpasswd
        Require valid-user
    </Directory>
</VirtualHost>
#######################
###       SSL       ###
#######################
<VirtualHost *:443>
```

```
        DocumentRoot "/var/www/vhost/domain.com/"
        ServerName domain.com
        ServerAlias www.domain.com
        ErrorLog logs/ssl_error_log
        TransferLog logs/ssl_access_log
        LogLevel warn
        SSLEngine on
        SSLProtocol All -SSLv2 -SSLv3 -TLSv1 -TLSv1.1
        SSLCipherSuite EECDH+AESGCM:EDH+AESGCM:AES256+EECDH:AES256+EDH
        SSLCertificateFile /var/www/vhost/ssl/domain/domain.crt
        SSLCertificateKeyFile /var/www/vhost/ssl/domain/domain.key
        SSLCertificateChainFile /var/www/vhost/ssl/domain/domain.ca-bundle

   <Directory /var/www/vhost/domain.com/>
        Options Indexes FollowSymLinks MultiViews
        AllowOverride All
   </Directory>
   <Directory "/var/www/vhost/domain.com/must_mysql">
        AuthType Basic
        AuthName "Restricted Content"
        AuthUserFile /etc/httpd/.htpasswd
        Require valid-user
    </Directory>
</VirtualHost>
```

Generating a .htpasswd:

```
htpasswd -c /var/www/vhost/domain.com/secure_domain username
```

Nginx vhost:

SSL+PHP7-fpm

```
server {
  listen 80;
  server_name www.domain.com;
  return 301 https://www.domain.com$request_uri;
}
```

```
server {
  listen 443 ssl;
  add_header Strict-Transport-Security "max-age=31536000; includeSubDomains" always;

  server_name www.domain.com;
  root /var/www/vhosts/domain/public;
  index index.php index.html;

  ssl on;
  ssl_certificate /etc/letsencrypt/live/www.domain.com/fullchain.pem;
  ssl_certificate_key /etc/letsencrypt/live/www.domain.com/privkey.pem;
  ssl_session_timeout 5m;
  ssl_ciphers 'EECDH+AESGCM:EDH+AESGCM:AES256+EECDH:AES256+EDH';
  ssl_protocols TLSv1 TLSv1.1 TLSv1.2;
  ssl_prefer_server_ciphers on;
  ssl_dhparam /etc/nginx/dh.pem;

  location / {
    try_files $uri $uri/ /index.php?$query_string;
  }

  location ~ \.php$ {
    include snippets/fastcgi-php.conf;
    fastcgi_pass unix:/run/php/php7.0-fpm.sock;
  }
}
```

Revese proxy

```
location / {
  proxy_pass_header Authorization;
  proxy_pass http://205.233.150.48:9099;
  proxy_set_header Host $host;
  proxy_set_header X-Real-IP $remote_addr;
  proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
  proxy_http_version 1.1;
  proxy_set_header Connection "";
  proxy_buffering off;
  proxy_request_buffering off;
  client_max_body_size 0;
```

```
  proxy_read_timeout 36000s;
  proxy_redirect off;
  proxy_ssl_session_reuse off;

}
```

Generate DH Key

```
openssl dhparam -out /etc/nginx/dh.pem 2048
```

Varnish

```
vim /etc/varnish/varnish.params
```

```
RELOAD_VCL=1
VARNISH_VCL_CONF=/etc/varnish/default.vcl
VARNISH_LISTEN_PORT=80
VARNISH_ADMIN_LISTEN_ADDRESS=127.0.0.1
VARNISH_ADMIN_LISTEN_PORT=6082
VARNISH_SECRET_FILE=/etc/varnish/secret
VARNISH_STORAGE="malloc,1G"
VARNISH_TTL=120
VARNISH_USER=varnish
VARNISH_GROUP=varnish
DAEMON_OPTS="-p thread_pool_min=5 -p thread_pool_max=500 -p thread_pool_timeout=300 -p
cli_buffer=16384 -p feature=+esi_ignore_other_elements -p vcc_allow_inline_c=on"
```

```
vim /etc/varnish/default.vcl
```

```
vcl 4.0;
backend default {
    .host = "127.0.0.1";
    #Change 8080 to httpd port
    .port = "8080";
}

sub vcl_recv {
}
```

```
sub vcl_backend_response {
}

sub vcl_deliver {
}
```

Apache reverse proxy (optional LDAP config)

```
#:httpd -M |grep ldap
ldap_module (shared)
authnz_ldap_module (shared)

## /etc/httpd/conf.d/*.conf <- default included

<Location />
    AuthType Basic
    AuthName "My AD"
    AuthBasicProvider ldap
    AuthLDAPBindDN "CN=$value1,OU=$value2,OU=$value3,DC=$value4,DC=$value5"
    AuthLDAPBindPassword "passhere"
    AuthLDAPURL
"ldaps://ip_here:636/OU=$value2,OU=$value3,DC=$value4,DC=$value5?sAMAccountName?sub?(&(objectC
ategory=person)(objectClass=user))"
    Require valid-user
</Location>



<VirtualHost *:80>
ProxyPreserveHost On
ProxyPass / http://127.0.0.1:8888/
ProxyPassReverse / http://127.0.0.1:8888/
</VirtualHost>

<VirtualHost *:443>
ProxyPreserveHost On
```

```
SSLEngine On
SSLCertificateFile /path/to/file
SSLCertificateKeyFile /path/to/file
ProxyPass / http://127.0.0.1:8888/ProxyPassReverse / http://127.0.0.1:8888/
```

Revision #7
Created 2017-07-09 13:36:18 UTC by Dave
Updated 2019-02-14 06:05:09 UTC by Carl