**nginx配置https**

**之前安装nginx时没有添加ssl模块，现在需要用https访问网站，则必须重新编译添加ssl模块**

**下载nginx源码包，解压**

**#yum –y install pcre-devel zlib-devel openssl openssl-devel**

1. 查看ngixn版本极其编译参数
   1. /usr/local/nginx/sbin/nginx –V
2. 进入nginx源码目录
   1. cd nginx-x.x.x
3. 以下是重新编译的代码和模块
   1. ./configure --prefix=/usr/local/nginx --with-http\_stub\_status\_module --with-http\_ssl\_module
4. make //千万别make install，否则就覆盖安装了
5. make完之后在objs目录下就多了个nginx，这个就是新版本的程序了
6. 备份旧的nginx程序
   1. cp /usr/local/nginx/sbin/nginx/usr/local/nginx/sbin/nginx.bak

提醒：然后将刚刚编译好的nginx覆盖掉原有的nginx（这个时候nginx要停止状态）

1. 把新的nginx程序覆盖旧的
   1. cp objs/nginx /usr/local/nginx/sbin/nginx
2. 测试新的nginx程序是否正确
   1. /usr/local/nginx/sbin/nginx -t
3. 启动nginx
   1. /usr/local/nginx/sbin/nginx
4. 平滑重启nginx
   1. /usr/local/nginx/sbin/nginx -s reload
5. 查看ngixn版本极其编译参数
   1. /usr/local/nginx/sbin/nginx -V
6. 修改Nginx配置文件，让其包含新标记的证书和私钥：

server {

        listen    443; //监听端口为443

        server\_name  www.localhost.cn;

        ssl   on;        　//开启ssl

        ssl\_certificate  /etc/pki/tls/certs/server.crt;     //证书位置

        ssl\_certificate\_key  /etc/pki/tls/certs/server.key;      //私钥位置

        ssl\_session\_timeout  5m;

        ssl\_protocols  SSLv2 SSLv3 TLSv1;       　　　　 //指定密码为openssl支持的格式

        ssl\_ciphers  HIGH:!aNULL:!MD5;              //密码加密方式

        ssl\_prefer\_server\_ciphers   on;

//依赖SSLv3和TLSv1协议的服务器密码将优先于客户端密码

        location / {

            root   html;                        //根目录的相对位置

            index  index.html index.htm;

         }

     }

平滑重启nginx服务器

/usr/local/nginx/sbin/nginx –s reload

另外还可以加入如下代码实现80端口重定向到443

server {

listen 80;

server\_name www.localhost.cn;

rewrite ^(.\*)$  https://$host$1 permanent;

}

通过以下配置，可以设置一个虚拟主机同时支持HTTP和HTTPS

listen 80;

listen 443 default ssl;

**同时支持80和443同时访问配置:**

server {

    listen      80 default backlog=2048;

    listen      443 ssl;

    server\_name  www.localhost.com;

    #ssl on;  //注释掉

    ssl\_certificate   /usr/local/https/www.localhost.com.crt;

    ssl\_certificate\_key  /usr/local/https/www.localhost.com.key;

    ssl\_session\_timeout 5m;

    ssl\_protocols TLSv1 TLSv1.1 TLSv1.2;

    ssl\_ciphers AESGCM:ALL:!DH:!EXPORT:!RC4:+HIGH:!MEDIUM:!LOW:!aNULL:!eNULL;

    ssl\_prefer\_server\_ciphers on;