SSL 安装配置指南

1. 购买 SSL 证书

首先，选择适合您需求的证书类型，并完成购买流程。购买后，您将获得证书文件和私钥文件。

2. 下载证书文件

在购买流程结束后，会提供一键下载证书文件的功能。请下载以下文件：

- 完整的证书链文件（例如：fullchain.pem）
- 私钥文件（例如：privkey.pem）

3. 配置 Nginx 服务器

接下来，您需要配置 Nginx 以使用新购买的 SSL 证书。

- 打开 Nginx 的配置文件。通常，您可以在/etc/nginx/sites-available/目录下找到默认的配置文件，或者您可能需要编辑特定的站点配置文件。使用文本编辑器打开配置文件，例如：

```
vim /etc/nginx/sites-available/default
```

或者，如果您有特定的站点配置文件：

```
vim  /etc/nginx/sites-available/your-site
```

- 在配置文件的 server 块中，找到 listen 指令，将其修改为使用 443 端口并启用 SSL，如下所示：

```
server {
    listen 443 ssl;
    server_name www.your-domain.com; # 替换为您的域名

    # SSL 证书配置
    ssl_certificate /path/to/your/fullchain.pem; # 替换为您的证书文件路径
    ssl_certificate_key /path/to/your/privkey.pem; # 替换为您的私钥文件路径

    # 其他 SSL 配置
    ssl_session_cache shared:SSL:10m;
    ssl_session_timeout  10m;
    ssl_ciphers HIGH:!aNULL:!MD5;
```

```
    ssl_prefer_server_ciphers on;

    # 其他配置...
}
```

- 确保替换/path/to/your/fullchain.pem 和/path/to/your/privkey.pem 为您实际证书文件的路径，以及 www.your-domain.com 为您的实际域名。

4. 重启 Nginx 服务

配置完成后，您需要重启 Nginx 服务以应用更改：

```
sudo systemctl restart nginx
```

5. 测试 SSL 证书

最后，使用浏览器访问您的网站，确保 HTTPS 连接正常工作。您可以通过 https://www.your-domain.com 访问您的网站（将 www.your-domain.com 替换为您的实际域名）。

6. 重定向 HTTP 到 HTTPS

为了确保所有用户都通过 HTTPS 访问您的网站，您可以配置 Nginx 将所有 HTTP 请求重定向到 HTTPS。

- 在相同的 Nginx 配置文件中，添加一个新的 server 块来处理 HTTP 请求的重定向：`server`

```
{
    listen 80;
    server_name www.your-domain.com; # 替换为您的域名
    return 301 https://$host$request_uri;
}
```

- 再次重启 Nginx 服务：`systemctl restart nginx`