链滴

在 Nginx/Tengine 服务器上安装证书

作者：Leif160519
原文链接：https://ld246.com/article/1566540774976
来源网站：链滴

<img src="https://ld246.com/images/img-loading.svg" alt="" data-src="">
本文摘自阿里云：<a href="https://ld246.com/forward?goto=https%3A%2F%2Fhelp.aliyun.co
%2Fdocument_detail%2F98728.html" target="_blank" rel="nofollow ugc">https://help.aliyun.
om/document_detail/98728.html
<blockquote>
原文中的某些 nginx 配置根据本人实际情况做了修改,故与原文有些出入。
</blockquote>
您可以从阿里云 SSL 证书服务控制台下载证书安装到您的 Nginx/Tengine 服务器上。
<h2 id="背景信息">背景信息</h2>
本文档以 CentOS 7、Nginx 1.15.6 为例。
本文档证书名称以 domain name 为示例，如证书文件名称为 domain name.pem，证书密钥
件名称为 domain name.key。
下载的 Nginx 证书压缩文件解压后包含：

.pem：证书文件。PEM 文件的扩展名为 CRT 格式。
.key：证书的密钥文件。申请证书时如果未选择自动创建 CRS，则下载的证书文件压缩包中不会
含.key 文件，需要您将自己手动常见的私钥文件拷贝到 cert 目录下。

<blockquote>
说明 .pem 扩展名的证书文件采用 Base64-encoded
的 PEM 格式文本文件，您可根据需要修改成其他扩展名。
证书的格式详见<a href="https://ld246.com/forward?goto=https%3A%2F%2Fhelp.aliyun.com
2Fknowledge_detail%2F42214.html" target="_blank" rel="nofollow ugc">主流数字证书都有哪
格式。
</blockquote>
<h2 id="操作指南">操作指南</h2>

登录阿里云 <a href="https://ld246.com/forward?goto=https%3A%2F%2Fyundunnext.con
ole.aliyun.com%2F%3Fp%3Dcasnext%23%2Foverview%2Fcn-hangzhou" target="_blank" rel=
nofollow ugc">SSL 证书控制台。

在 SSL 证书页面，点击已签发标签，定位到需要下载的证书并单击证书卡片右下角的下载打开
书下载对话框。
<a href="https://ld246.com/forward?goto=http%3A%2F%2Fstatic-aliyun-doc.oss-cn-hangzh
u.aliyuncs.com%2Fassets%2Fimg%2F66002%2F156274614339176_zh-CN.jpg" target="_blank"
rel="nofollow ugc"><img src="https://ld246.com/images/img-loading.svg" alt="null" data-sr
="http://static-aliyun-doc.oss-cn-hangzhou.aliyuncs.com/assets/img/66002/15627461433917
_zh-CN.jpg">

在证书下载对话框中定位到 Nginx/Tengine 服务器，并单击右侧操作栏的下载将 Nginx 版证书
缩包下载到本地。

解压 Nginx 证书。
您将看到文件夹中有 2 个文件：

证书文件（以.pem 为后缀或文件类型）
密钥文件（以.key 为后缀或文件类型）

<a href="https://ld246.com/forward?goto=http%3A%2F%2Fstatic-aliyun-doc.oss-cn-ha
gzhou.aliyuncs.com%2Fassets%2Fimg%2F66002%2F156274614333690_zh-CN.png" target="_

lank" rel="nofollow ugc"><img src="https://ld246.com/images/img-loading.svg" alt="null" data-src="http://static-aliyun-doc.oss-cn-hangzhou.aliyuncs.com/assets/img/66002/15627461433690_zh-CN.png">

在 Nginx 安装目录下创建 cert 目录，并将下载的证书文件和密钥文件拷贝到 cert 目录中。

<blockquote>
说明 如果您在申请证书时选择手动创建 CSR 文件，请将对应的密钥文件到 cert 目录中，并命名为 domain name.key。
</blockquote>
6.打开 Nginx 安装目录 > conf 文件夹 > nginx.conf 文件，在 nginx.conf 文件中找到以属性：
<pre><code class="highlight-chroma"># HTTPS server
server {
    listen 443 ssl http2 default_server;
    listen [::]:443 ssl http2 default_server;
    server_name _;
    root /usr/share/nginx/html;
    ssl_certificate "/etc/pki/nginx/server.crt";
    ssl_certificate_key "/etc/pki/nginx/private/server.key";
    ssl_session_cache shared:SSL:1m;
    ssl_session_timeout 10m;
    ssl_ciphers HIGH:!aNULL:!MD5;
    ssl_prefer_server_ciphers on;
    # Load configuration files for the default server block.
    include /etc/nginx/default.d/*.conf;

    location / {
    }

    error_page 404 /404.html;
    location = /40x.html {
    }

    error_page 500 502 503 504 /50x.html;
    location = /50x.html {

    }
}
</code></pre>
修改 nginx.conf 文件如下：
<pre><code class="highlight-chroma">#以下属性中以ssl开头的属性代表与证书配置有关，其他属性请根据自己的需要进行配置。
server {
    listen 443;
    server_name localhost; # localhost修改为您证书绑定的域名。
    ssl on; #设置为on启用SSL功能。
    ssl_certificate /etc/nginx/ssl/domain name.pem; #将domain name.pem替换成您证书的文件名。
    ssl_certificate_key /etc/nginx/ssl/domain name.key; #将domain name.key替换成您证书的密钥文件名。
    ssl_session_timeout 5m;
    ssl_ciphers ECDHE-RSA-AES128-GCM-SHA256:ECDHE:ECDH:AES:HIGH:!NULL:!aNULL:!MD5:!ADH:!RC4; #使用加密套件。
    ssl_protocols TSv1 TLSv1.1 TLSv1.2; #使用该协议进行配置。
    ssl_prefer_server_ciphers on;
    root /usr/share/nginx/html; #站点目录。

    location / {
        index index.html index.htm;
    }

    error_page 404 /404.html;
    location = /40x.html {
    }

    error_page 500 502 503 504 /50x.html;
    location = /50x.html {
    }
}

</code></pre>
<blockquote>
注意：若有多个域名指向同一台服务器 IP 地址，则复制上述配置，粘贴在下方，改一下对应的 <code>server_name</code>,证书地址和证书名称即可
</blockquote>
7.保存 nginx.conf 文件后退出。
8.重启 Nginx 服务器。
<blockquote>

说明 如果您有配置多个虚拟主机 Include conf/vhost，参考虚拟主机配置 SSL 证书进行配置。<
p>
</blockquote>
9.（可选步骤）设置 http 请求自动跳转 https。
在需要跳转的 http 站点下添加以下 rewrite 语句，实现 http 访问自动跳转到 https 页面
<pre><code class="highlight-chroma"><span class="highlight
cl">server {
    listen 80 defaul
_server;
    listen [::]:80 def
ult_server;
    server_name _;
    #实现http访问
动跳转到https页面
    rewrite ^(.*)$ ht
ps://$host$1 permanent;
    root /usr/share
nginx/html;
    # Load configu
ation files for the default server block.
    include /etc/ng
nx/default.d/*.conf;
    location / {
    }

    error_page 404
404.html;
    location = /40x
html {
    }

    error_page 500
502 503 504 /50x.html;
    location = /50x
html {
    }
}

</code></pre>
<h2 id="虚拟主机配置SSL证书">虚拟主机配置 SSL 证书</h2>
1.打开虚拟主机配置文件 vhost.conf 或*.conf，复制以下内容粘贴到下方位置、将端口改为 443
https 默认端口）并增加证书相关配置。
<pre><code class="highlight-chroma">>><span class="highlight
cl">server {
>   listen 80;
>   server_name lo
alhost ;
>   location / {
>   index index.h
ml index.htm;
>   }
>}
>
>server {

```
</span></span><span class="highlight-line"><span class="highlight-cl">    listen 443;
</span></span><span class="highlight-line"><span class="highlight-cl">    server_name lo
alhost;
</span></span><span class="highlight-line"><span class="highlight-cl">    ssl on;
</span></span><span class="highlight-line"><span class="highlight-cl">    ssl_certificate ce
t/domain name.pem; #将domain name.pem替换成您证书的文件名。
</span></span><span class="highlight-line"><span class="highlight-cl">    ssl_certificate_k
y cert/domain name.key; #将domain name.key替换成您证书的密钥文件名。
</span></span><span class="highlight-line"><span class="highlight-cl">    ssl_session_tim
out 5m;
</span></span><span class="highlight-line"><span class="highlight-cl">    ssl_ciphers EC
HE-RSA-AES128-GCM-SHA256:ECDHE:ECDH:AES:HIGH:!NULL:!aNULL:!MD5:!ADH:!RC4;
</span></span><span class="highlight-line"><span class="highlight-cl">    ssl_protocols T
Sv1 TLSv1.1 TLSv1.2;
</span></span><span class="highlight-line"><span class="highlight-cl">    ssl_prefer_serve
_ciphers on;
</span></span><span class="highlight-line"><span class="highlight-cl">    location / {
</span></span><span class="highlight-line"><span class="highlight-cl">        index index.h
ml index.htm;
</span></span><span class="highlight-line"><span class="highlight-cl">    }
</span></span><span class="highlight-line"><span class="highlight-cl">}
</span></span></code></pre>
<p>2.保存 nginx.conf 文件后退出。</p>
<p>3.重启 Nginx 服务器。</p>
<p>安装证书相关文档：</p>
<ul>
<li><a href="https://ld246.com/forward?goto=https%3A%2F%2Fhelp.aliyun.com%2Fdocum
nt_detail%2F98576.html%23concept-omf-lxn-yfb" title="您可以将下载的证书安装到Tomcat服
器上。Tomcat支持PFX格式和JKS两种格式的证书，您可根据您Tomcat的版本择其中一种格式的证
安装到Tomcat上。" target="_blank" rel="nofollow ugc">在 Tomcat 服务器上安装 SSL 证书</a
</li>
<li><a href="https://ld246.com/forward?goto=https%3A%2F%2Fhelp.aliyun.com%2Fdocum
nt_detail%2F98727.html%23concept-zsp-d1x-yfb" title="您可以将从阿里云SSL证书控制台下载
证书安装到您的Apache服务器上，使Apache服务器支持 HTTPS安全访问 。" target="_blank" rel=
nofollow ugc">在 Apache 服务器上安装 SSL 证书</a></li>
<li><a href="https://ld246.com/forward?goto=https%3A%2F%2Fhelp.aliyun.com%2Fdocum
nt_detail%2F102450.html%23concept-cfn-yf2-kgb" title="本文档为您介绍了如何在Ubuntu系统
及Apache2中安装阿里云SSL证书。" target="_blank" rel="nofollow ugc">Ubuntu 系统 Apache 2
部署 SSL 证书</a></li>
<li><a href="https://ld246.com/forward?goto=https%3A%2F%2Fhelp.aliyun.com%2Fdocum
nt_detail%2F42215.html%23concept-ccz-hcv-ydb" target="_blank" rel="nofollow ugc">我获
到的数字证书如何配置在自己的 Apache 中？</a></li>
<li><a href="https://ld246.com/forward?goto=https%3A%2F%2Fhelp.aliyun.com%2Fdocum
nt_detail%2F98729.html%23concept-ntq-f1x-yfb" title="您可将下载的阿里云SSL证书安装到IIS
务器上，使您的IIS服务器支持HTTPS安全访问。" target="_blank" rel="nofollow ugc">在 IIS 服
器上安装证书</a></li>
<li><a href="https://ld246.com/forward?goto=https%3A%2F%2Fhelp.aliyun.com%2Fdocum
nt_detail%2F102939.html%23concept-i2b-cdb-mgb" title="本文档介绍了CentOS系统下Tomcat
8.5或9部署SSL证书的操作说明。" target="_blank" rel="nofollow ugc">CentOS 系统 Tomcat 8.5
9 部署 SSL 证书</a></li>
<li><a href="https://ld246.com/forward?goto=https%3A%2F%2Fhelp.aliyun.com%2Fdocum
nt_detail%2F63624.html%23concept-jrz-bbw-ydb" target="_blank" rel="nofollow ugc">Jetty
服务器配置 SSL 证书</a></li>
</ul>
```

<blockquote>
注意：若 nginx 版本在 1.15 之后，请将 <code>ssl on;</code> 设置为 <code> listen 443 ssl
</code> 即可
</blockquote>
<pre><code class="highlight-chroma"><span class="highlight
cl">server {
    listen 443 ssl;
    server_name leif
fun;
    #ssl on;
…
</code></pre>