



enjoy器士

码龄8年

暂无认证

410 2万+ 5008 29万+  
原创 周排名 总排名 访问 等级

6311 93 74 44 467  
积分 粉丝 获赞 评论 收藏



私信

关注

搜博主文章

热门文章

Linux 动态加载并调用动态库(.so)方法介绍  
22372

c++ 实现http或者https通信 20930

解决Nginx编译时 openssl not found问题  
13463

MFC 加载并显示图片 10677

springboot 之 指定mybatis中mapper文件  
扫描路径 6145

最新评论

一台nginx并发测试  
lonju: 我是您的粉丝,我想跟您学技术,能  
留个联系方式吗

VC++ 之 release版本不生成pdb文件  
周健文: 由debug换成release之后,启动程  
序报ucrtbase.pdb错误,后来在release...

MFC 加载并显示图片  
Allen Roson: 很全,学习了

springboot 之 开发中遇到的问题(一)  
Tisfy: 厉害厉害

webflux 之 常用变量说明  
golang人工智能框架: go更加方便些,也灵  
活,性能看人的水平了

您愿意向朋友推荐“博客详情页”吗?



强烈不推荐 不推荐 一般般 推荐 强烈推荐

## SSL双向认证的认证模式设置问题

原创 enjoy器士 2017-11-23 17:05:20 5239 收藏 7

分类专栏: SSL 文章标签: SSL openssl



SSL 专栏收录该内容

0 订阅

6 篇文章

订阅专

栏

今天介绍一下SSL双向认证服务器端认证模式的设置,很关键。

初始化ssl时,要使用SSL\_CTX\_set\_verify函数设置验证模式,下面介绍下集中模式:

### OpenSSL 验证证书模式

OpenSSL 有四种验证证书的模式,这样可以自己根据验证结构来决定应用程序的行为。四种验证模式分别是:

- SSL\_VERIFY\_NONE: 完全忽略验证证书的结果。当握手必须完成的话,就选中这个选项。其实真正有证书的人很少,尤其是在中国,那么如果 SSL 运用于一些免费的服务,比如 EMAIL 的时候,SERVER 端最好采用这个模式。
- SSL\_VERIFY\_PEER: 希望验证对方的证书。这个是最一般的模式。对 CLIENT 来说,如果设置了这样的模式,验证 SERVER 的证书出了任何错误,SSL 握手都告吹。对 SERVER 来说,如果设置了这样的模式,CLIENT 倒不一定要把自己的证书交出去。如果 CLIENT 没有交出证书,SERVER 自己决定下一步怎么做。
- SSL\_VERIFY\_FAIL\_IF\_NO\_PEER\_CERT: 这是 SERVER 使用的一种模式,在这种模式下,SERVER 会向 CLIENT 要证书。如果 CLIENT 不给,SSL 握手告吹。
- SSL\_VERIFY\_CLIENT\_ONCE: 这是仅能使用在 SSL\_SESSION\_RENEGOTIATION 阶段的一种方式。如果不是用这个模式的话,那么在 RENEGOTIATION 的时候,CLIENT 都要把自己的证书送给 SERVER,然后做一番分析。这个过程很消耗 CPU 时间的,而这个模式则不需要 CLIENT 在 RENEGOTIATION 的时候重复送自己的证书了。



enjoy器士

关注

4

0

7



专栏目录

### 双向SSL认证配置说明

10-18

双向SSL认证配置说明,结合数字证书,实现服务器与客户端双向安全通信认证。

### SSL认证流程(单向认证和双向认证)

毛毛虫的博客 1133

一、单向认证 客户端认证服务器(常用的认证方式) 二、双向认证 客户端和服务端双向认证



优质评论可以帮助作者获得更高权重

抢沙发



评论

### HTTPS双向认证配置\_Yong Ledo的博客

9-29

服务端需要获取到客户端通过浏览器发送过来的认证证书,如:该证书在服务端的证书库中已存在,仅仅是个匹配过程,匹配成功即通过认证,可继续访问网站...

### ssl证书双向认证失效的一种解决方案\_HRay's blog

9-30

ssl证书双向认证配置可参考http://blog.csdn.net/hrayha/article/details/46446653 某天突然发现证书认证失效了,所有人访问都校验失败,提示400错误,服务...

### TLS/SSL 协议详解(25) https双向认证及常见问题总结

Network/Storage/Linux Kernel 9355

分类专栏

Spring全家桶 78篇

高可用和负载均衡 9篇

服务器并发 3篇

工具及公共库 3篇

JavaScript 4篇

java 30篇

MQ 7篇

杂谈八卦 10篇

网络传输协议 10篇

缓存 1篇

数据库及相关中间件 50篇

React+Antd 5篇

桌面开发工具 20篇

学习指引 4篇

分布式系统 5篇

服务器架构 5篇

YAML 1篇

java集合 5篇

微服务 2篇

监控 4篇

算法 10篇














开源 1篇

JVM 16篇

设计模式 2篇

最新文章			
一台nginx并发测试			
Windows C盘占用内存与实际内存不符合			
windows磁盘分析工具SpaceSniffer			
2021			
09月 5篇	08月 10篇	07月 5篇	06月 2篇
05月 3篇	04月 14篇	03月 22篇	02月 8篇
01月 16篇			
2020年 240篇	2019年 106篇		
2018年 10篇	2017年 12篇		

Tomcat双向认证SSL证书	08-16
个人学习笔记，markdown风格，记录Tomcat双向认证SSL证书的过程	
Nginx https(SSL)双向认证配置_Fighter168的专栏	9-27
Nginx https(SSL)双向认证配置 基于Let's Encrypt证书和自签名证书实现双向认证。使用Let's Encrypt实现客户端对服务端的验证,利用自签名证书完成服...	
SSL双向认证-补坑篇_bigwood99的博客	9-19
SSL双向认证-补坑篇 以下内容转自:互联网内容,但雷同太多无从知晓院创作者。本文意在补充不完整部分,如果原创者不希望引用,请联系本人,会立即删...	
易语言SSL双向认证源码	07-20
易语言SSL双向认证源码,SSL双向认证,设置证书文件,连接,取Socket句柄,建立SSL连接,断开连接,取服务器IP,发送数据,取回数据,取消息类型,标记参数是否...	
curl_opt_ssl_verifypeer后https还是验证不过_2020CNAS能力验证小总结	weixin_42327291的博客 247
喜欢就关注我们吧！提前祝大家中秋节加国庆节快乐每年的这个时候，都要迎来三所的实验室能力验证，今年也不例外。在毫无准备的情况下，下载了服...	
https 双向认证基本配置学习 - pzzqingchong的专栏 - CSDN博客	11-5
其他PKCS格式标准本人未深入了解,这里介绍的三种是配置https双向认证(pkcs10,pkcs#12) 以及非对称加密解密(pkcs8) 时使用到的。1.4 小结本次app ...	
SSL单向/双向认证详解(其实是握手过程的详解)_legend_x...	10-9
@SSL 的握手部分结束,SSL 安全通道的数据通讯开始,客户和服务器开始使用相同的对称密钥进行数据通讯,同时进行通讯完整性的检验。 双向认证 SSL ...	
Python数据抓取出现错误"[SSL: CERTIFICATE_VERIFY_FAILED] certificate verify failed (_ssl.c:841) None"问...	干勾鱼的CSDN博客 7717
转载请注明出处：http://blog.csdn.net/dongdong9223/article/details/85232283 本文出自【我是干勾鱼的博客】 Ingredients：Language Python：Pytho...	
Java ssl socket 双向认证	04-18
NULL 博文链接：https://1002878825-qq-com.iteye.com/blog/1838805	
SSL双向认证原理以及期间证书的使用_刘春明的博客	8-11
SSL双向认证原理以及期间证书的使用 原理 要想弄明白SSL认证原理,首先要对CA有所了解,它在SSL认证过程中有非常重要的作用。说白了,CA就是一...	
SSL双向认证(高清版)_weixin_30371875的博客	10-3
介绍了SSL双向认证的一些基本问题,以及使用Nginx+PHP基于它搭建https的Webservice。 之前的方式只是实现1:1的模式,昨天同事继续实现了n:1的模式,...	
浅析打开eclipse出现Incompatible JVM的解决方法	09-05
本篇文章是对打开eclipse出现Incompatible JVM的解决方法进行了详细的分析介绍，需要的朋友参考下	
JAVA实现的SSL/TLS双向认证源代码	02-02
压缩包里有客户端源码和服务器端源码，支持TCP的双向认证，也支持WEBSOCKET的双向认证，内附测试wss的测试例子，需要生成PKCS12的证书，...	
C语言写的带有头结点的链表	04-03
这是一个带有头结点的链表，实现了链表的创建，翻转和销毁。并在main（）函数中举例测试。	
netty的SSL双向认证	01-18
netty的client和server端建立SSL连接，并进行双向的证书验证	
linux环境下ssl多线程编程实例（整理）	guozhiyingguo的博客 2794
服务端：#include #include #include #include #ifndef _WIN32 #include #include #include #include #include #include #include #else #include #include #endif #...	
SSL原理介绍	u013673367的专栏 4527
SSL原理介绍 SSL——安全套接字层（Secure Sockers Layer）协议由著名的Netscape公司开发。为了保证通信双方建立安全可靠的传输隧道，SSL使用...	
联盟链系列 - Https双向验证	搬砖魁首的博客 385
boost 实现双向认证解决办法 boost::asio::ssl::context 要与OpenSSL进行相互认证，必须在客户端使用SSL_VERIFY_PEER在服务器端使用SSL_VERIFY...	
openssl详解 热门推荐	王宁的博客 1万+
OpenSSL简介 目录 目录 第一章 前言 第二章 证书 第三章 加密算法 第四章 协议 第五章 入门 第六章 指令 verify 第七章 指令asn1parse 第八章 指令CA（...	
©2021 CSDN 皮肤主题: 技术黑板 设计师:CSDN官方博客 返回首页	

 Android	1篇
 Python	1篇
 docker	2篇
 FastDFS	1篇
 webflux	6篇
 C++	28篇
 STL	12篇
 Linux	31篇
 SSL	6篇
 c#	1篇
 windows	49篇
 Golang、PHP、Pytho...	8篇
 编译配置	3篇
 不知道怎么分类的文章	10篇



