

最后更新时间: 2010年12月22日

软件版本号: linux Nginx0.7稳定版 openss1-0.9.8 ActivePer1-5.12.2 VC++6.0

服务器证书安装配置指南系列之

Nginx 服务器证书安装配置指南

TTT. CANIC. CA

中国互联网络信息中心(CHNIC)

地址:北京中关村南四街四号中国科学院软件园1号樓一层 7*24小时客户服务咨询电话:86-10-58813000 传真:86-10-58812666 邮政地址:北京349信箱6分箱 CMMIC 邮政编码:100190

中国互联网络信息中心 HTTP://WWW.CNNIC.CN

目录

1.	应用]环境	3
2.	关于	openssl	3
	2.1	openssl 简介	3
	2.2	openssl 下载及安装配置	3
3.	申请	f服务器证书	4
	3.1	生成私钥	4
	3.2	生成 csr 请求文件	4
4.	下载	成服务器证书	6
	4.1	准备下载证书所需信息	6
	4.2	下载证书	6
5.	安装	根证书和服务器证书	11
	5.1	下载根证书和 CNNIC 中级根证书	11
6.	修改	z配置文件	14
	6.1	修改Nginx SSL配置	15
7.	备份)服务器证书	15

图表目录

图表一	生成密钥命令行	4
图表二	生成 csr 请求文件	4
图表三	查看 csr 文件	6
图表四	可信服务器证书下载页面	7
图表五	填入收到的参考号和授权码以及生成的csr	8
图表六	生成证书	9
图表七	格式转换	10
图表八	证书导出向导	11
图表九	查看根证书 roottest.cer	12
图表十	查看中级根证书 cnnic.cer	13
图表十一	一 证书导出向导(B)	14
中国互联网络	络信息中心	2/15

1. 应用环境

系统环境: windows xp sp3; Nginx; openssl-0.9.8; Perl-5.12.2; vc++6.0. 证书类型: 可信服务器证书,申请地址: http://www.cnnic.cn/jczyfw/wzws/

2. 关于 openss1

1) openss1 简介

openssl 是一个 Linux/windows 平台下、开放源代码的实现了 SSL 及相关加密 技术的软件包。

2) openssl 下载及安装配置

配置 OPENSSL_CONF 的变量环境,值为 openssl 里 apps 目录下的 openssl.cnf 文件。

安装 perl 和 vc6, 注册环境变量。

然后运行 cmd 进入到 Openssl 根目录,输入 perl Configure VC-WIN32,回车输入 ms\do_ms,然后 cd 到 microsoft visual studio\vc98\bin 目录下执行 vcvars32.bat, 最后回到 openssl 目录下执行 nmake -f ms\ntdll.mak 成功之后在 openssl 安装目 录下多了几个文件夹并且文件夹下有相关文件。需要把得到的 out32dll 文件夹路 径添加到变量环境 path 里。

以上是配置 openssl。

3. 申请服务器证书

本手册以 m1.cnnic.cn 为例,以下命令请使用 开始-运行-cmd 进入 DOS 环境进行

1) 生成私钥

命令格式: openssl genrsa -des3 -out cnnic.key 2048

注: []中的内容为需要输入的参数

● keystore_name: 表示证书密钥库的文件名, 扩展名一般为 key

如下图所示:

图表一 生成密钥命令行

如上图所示,行命令运后会提示输入两次私钥的密码,结果生成 2048 位的 RSA 私钥,私钥文件名为: m1. cnnic. cn. key。

<注: CNNIC 可信服务器证书要求域名证书密钥对最少为 2048 位>

2) 生成 CSR 证书请求文件

命令格式: openssl req -new -key ssl.key -out cnnic.csr

注: []中的内容为需要输入的参数

● csr_name: 表示生成的证书请求文件的文件名

● keystore_name: 表示证书密钥库的文件名, 扩展名一般为 key

如下图所示:

E:\openssl\openssl-0.9.8>openssl req -new -key m1.cnnic.cn.key -out m1.cnnic. csr Enter pass phrase for m1.cnnic.cn.key: You are about to be asked to enter information that will be incorporated into your certificate request. What you are about to enter is what is called a Distinguished Name or a DN. There are quite a few fields but you can leave some blank For some fields there will be a default value, If you enter '.', the field will be left blank. Country Name (2 letter code) [AU]:CN State or Province Name (full name) [Some-State]:beijing Locality Name (eg, city) []:beijing Organization Name (eg, company) [Internet Widgits Pty Ltd]:cnnic Organizational Unit Name (eg, section) []:cnnic Common Name (eg, YOUR name) []:m1.cnnic.cn Email Address []: Please enter the following 'extra' attributes to be sent with your certificate request A challenge password []: An optional company name []: E:\openss1\openss1-0.9.8>

图表二 生成 csr 请求文件

上述命令运行后,系统提示输入第一步骤中输入的私钥密码,然后输入 X. 509 证书所要求的字段信息,包括国家(中国添 CN)、省份、所在城市、单位名称、单位部门名称(可以不填直接回车)。请注意:除国家缩写必须填 CN 外,其 余都可以是英文或中文。

Common Name 项请输入您要申请域名证书的域名,例如:如果需要为 www.domain.cn申请域名证书就必须输入www.domain.cn而不能输入domain.cn。 通配域名证书请填写通配域名;多域名证书仅需要填写第一个域名名称即可。

请不要输入 Email、口令(challenge password)和可选的公司名称,直接打 回车即可。

现在已经成功生成了私钥文件:ml.cnnic.cn.key 保存在您的服务器中。生成的 csr 文件为文本文件,可以使用记事本等文本查看工具打开刚刚生成的证书

请求文件,如下图所示:

🖹 E:\openssl\openssl-0.9.8\m1.cnnic.cn.csr - Notepad++ 🛛 🔤 🗖 🗖		
文件 (2)	编辑 @) 搜索 @) 视图 (V) 格式 @) 语言 @) 设置 @) 宏 @) 运行 ®) TextFX 插件 @) 窗口 (M) <u>?</u> X	
🗋 占) 🗄 🖻 🕞 🕞 🖕 🖌 🕞 💼 Ə C 🃾 🍢 🍕 👒 🖫 🖼 🚍 1 運 💌 🕨 💌 🖼 🕿 🐣	
🚍 m1. (ennie. en. esr	
1	BEGIN CERTIFICATE REQUEST	
2	MIICrDCCAZQCAQAwZzELMAkGA1UEBhMCQ04xEDAOBgNVBAgTB2J1aWppbmcxEDAO	
3	${\tt BgNVBAcTB2JlaWppbmcxDjAMBgNVBAoTBWNubmljMQ4wDAYDVQQLEwVjbm5pYzEU}$	
4	MBIGA1UEAxMLbTEu¥25uaWMu¥24wggEiMAOGCSqGSIb3DQEBAQUAA4IBDwAwggEK	
5	loIBAQCwZKe5sIA8Vv7uYleWQMUVOS7K/dagHhyb9DYKOuOSQqJkHsFzAMUZzyjL	
6	kvE2tUTNtMqbPAxV8TGSG+AcC7zNABydQpAUWw91dGoLqGtkdtOsQ/tWd0Bbi10j	
7	8amCi/yRxkpPSPJPrLisBFCxwt+8wGj8WICj3vP8j0qnpUtkfx3S9AMfaAveGret	
8	lUF/80DBboVwJXCTKwwc+dHykjsiswAOiWYlgnArdexn1gR4Ym59IjiFmOfiiBSK	
9	bGwV1NXJ21f6DsLFKf8JvZq9Yfdjc135QQPOpzGhR98TKzSTv/6/c+ocG2yexgFt	
10	MZac/Z4lJh9iUmNkp69nbs1sHU5FAgMBAAGgADANBgkqhkiG9w0BAQUFAAOCAQEA	
11	qGbSXekMJTPsS7VHuP1YzpkOaXN3D3AAyOoT7MC3pEDnlk49e779Vxr2Bl3nFbh1	
12	4P5exg01f20i60UeCEOh45sMgFCGnocGf/rQJgmBFIuGiuKbWAtzSj/4zVjKw/wp	
13	TrDhVYRMIfipMeL/k/gny99TesmcaGdlBvJs9MTEEHk+8HPXWLH1rEzE4i08Q8+g	
14	lkkn/ormacYh3rxez+3wdxLIABP+YYONqPlvaVcD/st4STWd5yL3U1PR2+WL251j	
15	LsSHH5pD+m0ZN/qKbkLLD74DwmmXMaUkH296I10IwEuG8oELpUUEb9iwLsCeQ4Fu	
16	yMh4nWxfCx1P7sLG59hpdA==	
17	END CERTIFICATE REQUEST	
18		
1		
Normal le	ength: 1005 lines: 18 Ln: 1 Col: 1 Sel: 0 UNIX ANSI INS	

图表三 查看 csr 文件

4. 下载服务器证书

1) 准备下载证书所需信息

参考号与授权码:参考号与授权码是下载证书的密码凭证。当申请的证书通 过审核时,用户将接收到由 CNNIC 发送的通过审批的电子邮件通知,该邮件中含 有 16 位的参考号与授权码信息,其中参考号与授权码的前 13 位为明文显示,后 3 位为密文显示。审核员会以邮件通知的方式发送后三位的明文显示。

2) 下载证书

登录 CNNIC 可信网络服务中心网页面

http://www.cnnic.cn/jczyfw/wzws/xz/201010/t20101027_16322.html,

点击页面中部的"可信服务器证书下载"链接进入到证书下载页面,如下图 所示:

	点击这里进行任线USB仪箍
参考号:	
授权码:	
	请把整个CSR文件中 BEGIN CERTIFICATE REQUEST 和 END CERTIFICATE REQUEST 之间的内容复制到下边的输入框中
证书请求文件(CSR):	

图表四 可信服务器证书下载页面

根据网页上的提示输入"参考号"和"授权码",将证书请求文件中除去头尾"-----BEGIN NEW CERTIFICATE REQUEST-----"和"-----END NEW CERTIFICATE REQUEST-----"和"-----END NEW CERTIFICATE REQUEST-----"的中间部分内容复制到 CSR 文本框中。结果如下所示:

	点击这里进行在线CSR校验
参考号:	MV4K646JDDHAF8W5
授权码:	CJQLNDB7FQSVEJA3
	请把整个CSR文件中 BEGIN CERTIFICATE REQUEST 和 END CERTIFICATE REQUEST 之间的内容复制到下边的输入框中
证书请求文件(CSR):	MIICrDCCAZQCAQAwZzELMAkGA1UEBhMCQO4xEDAOBgNVBAgTB 2J1aWppbmcxEDAO BgNVBAcTB2J1aWppbmcxDjAMBgNVBAoTBWNubm1jMQ4wDAYDV QQLEwVjbm5pYzEU MBIGA1UEAxMLbTEuY25uaWMuY24wggEiMAOGCSqGSIb3DQEBA QUAA4IBDwAwggEK AoIBAQCw2Ke5sIA8Vv7uY1eWQMUVOS7K/dagHhyb9DYKOuOSQ qJkHsFzAMUZzyjL kvE2tUTNtMqbPAxV8TGSG+AcC7zNABydQpAUWw91dGoLqGtkd tOsQ/tWdOBbi10j 8amCi/yRxkpPSPJPLisBFCxwt+8wGj8WICj3vP8jOqnpUtkf x3S9AMfaAveGret 1UF/80DBboVwJXCTKwwc+dHykjsiswAOiWY1gnArdexn1gR4Y
	m59IjiFmOfiiBSK bGwV1NXJ21f6DsLFKf8JvZq9Yfdjc135QQPOpzGhR98TKzSTv /6/c+ocG2yexgFt MZac/Z41Jh9iUmNkp69nbs1sHU5FAgMBAAGgADANBgkqhkiG9 wOBAQUFAAOCAQEA qGbSXekMJTPsS7VHuP1YzpkOaXN3D3AAyOoT7MC3pEDn1k49e 779Vxr2B13nFbh1

图表五 填入收到的参考号和授权码以及生成的 csr

点击"提交",如果参考号、授权码和 CSR 均无问题,则显示页面如下所

示:



图表六 生成证书

请按页面提示保存,文件名保存为 m1. cnnic. cn. cer。该文件即为申请的证书,如果该证书丢失,就必须进行证书补办。

注意:关于证书的格式转换

从 CNNIC 获得的证书格式为 X509 格式。该将证书文件的扩展名由 txt 改为 cer 或 crt 后,可在 windows 中双击打开查看证书的相关信息。显示信息类 似 下图所示:

证书 ? 🔀	
常规 详细信息 证书路径	
正书信息	
Tindows 没有足够信息,不能验证该证书。	
褒发给 : m1. cnnic. cn	
価发表: apping root	
有效起始日期 2010-12-8 到 2011-12-8	
「存地対かっ」「「病失去消弭」の」	
女表址やせい 」 「	

图表七 格式转换

X509 格式的证书利用 windows 提供的图形界面操作工具可以另存为以下两种编码格式:

- BASE64 编码格式: 该格式的证书可以用记事本打开
- DER 编码格式:二进制格式

在上图中,点击"详细信息"->"复制到文件"后,即可以根据提示点击"下 一步"利用证书导出向导导出需要格式的证书,如下图所示:

· 证书导出向导 🛛 🛛 🔀	
导出文件格式 可以用不同的文件格式导出证书。	
选择要使用的格式:	
● DER 编码二进制 X.509 (CER) (D)	
○Base64 编码 X.509 (.CER) (<u>S</u>)	
◯加密消息语法标准 - PKCS #7 证书(.P7B)(C)	
○私人信息交换 - PKCS #12 (.PFX)(P)	
启用加强保护(要求 IE 5.0, NT 4.0 SP4 或更高版本)(E)	
□ 如果导出成功,删除密钥 Œ)	
〈上一步 @)下一步 @)〉 取消	

图表八 证书导出向导(A)

5. 安装根证书和服务器证书

1) 下载根证书及CNNIC中级根证书

下载地址:

快速证书: <u>http://www.cnnic.cn/jczyfw/wzws/ksym/ksxz/201105/t20110524_21055.html</u>

标准证书: <u>http://www.cnnic.cn/jczyfw/wzws/bzkx/xz/201010/t20101027_16322.html</u>

EV证书: <u>http://www.cnnic.cn/jczyfw/wzws/kxEV/xz/</u>

将 CNNIC 中级根证书文件名保存为 "CNNIC. cer",将根证书文件名保存为 "root. cer"。

	🖀 C:\Documents and Settings\Administrator\桌面\roottest.cer - Wotepad++ 🛛 🔳 🗖 🗙		
Γ	文件 (2))编辑(E)搜索(S)视图(V)格式(W)语言(L)设置(E)宏(D)运行(B) TextFX 插件(E)窗口(W)?	X
			Z »
1	😑 roo	ottest. cer	
	1	BEGIN CERTIFICATE	
	2	MIIDVTCCAj2gAwIBAgIENJwAATANEgkqhkiG9w0BAQUFADAyMQswCQYDVQQGEwJj	
	3	bjEOMAwGA1UEChMFY25uaWMxEzAREgNVBAMTCmNubmljIHJvb3QwHhcNMDcwNDI4	
	4	MDY1MzUOWhcNMjcwNDI4MDY1MzUOWjAyMQswCQYDVQQGEwJjbjEOMAwGA1UEChMF	
	5	Y25uaWMxEzARBgNVBAMTCmNubmljIHJvb3QwggEiMAOGCSqGSIb3DQEBAQUAA4IB	
	6	DwAwggEKAoIBAQCIX7mxu4SewGcOR2yTwMc7Jpnb/dSZ3R0QmpNzvYXiow+rQI9p	
	7	Jbe/QDR1W05NPco13B118WsPIiyyGrKFNZeU7eDtD8DWMySD1z5HHFTiIp051Zsx	
	8	3Lihs3GXoGNs31lQ47Tj8rbhidYCV5+1n5wTPmZtdlMuuJW6BT/7l0vHcxk56ufi	
	9	U356Zj9RCyWgTODr8Bjx7tgp/fD1E2iDXLU139McJ3wINtAImkPdySWQ1Y7aCcPt	
	10	$\tt mtLogYtswXZDfD7wWBaXEb3b50yE41KEwh7XjqQZc8hqTcsZFJxLdQkFd1CN5hww$	
	11	eU2akEdIaPkLouF/eTywp/lsZfW/7jHzSBuJlgMBAAGjczBxMBEGCWCGSAGG+EIB	
	12	AQQEAwIABzAfBgNVHSMEGDAWgBT/aHinz7qOO3IljarQW6XOkNDOvzAPBgNVHRMB	
	13	$\tt Af8EBTADAQH/MAsGA1UdDwQEAwIB/jAdBgNVHQ4EFgQU/2h4p8+6tDtyJY2q0Fu1$	
	14	9JDQ9L8wDQYJKoZIhvcNAQEFBQADggEBAEgXsvAa218q73Lw8qQhF24oaUqxpXi5	
	15	IWQe1NATjxO2G9jnvLXWAeQ4LFyqA7LPyQJf2auucAPoWNV4gqsMcWKXXcmv4rAi	
	16	DtRr3D273HJERfludU/jFh0ZQy4N0U2a+rq6eoKC/biCqu8iZlfayJ7hWPPJDQ4e	
	17	FuB70IyV7aEeDAlYjk5ZnP4+EMcvY0sNaeOgnCFsSC1HzP8pYfsk7RrXHPZI+Gy5	
	18	2YTrrVeWrKCPlys3QLj2UojjayOKiZHnrknjZLnj1OI+XjFAFm8pe38sTbeRlrka	
	19	p1o40wmVjavIEQuPY1Up6DLa4fJ6VLpqmvTT+j6Mokb2h+0Zrs05HDM=	
	20	END CERTIFICATE	
	21		
1	formal 1	length : 1236 lines : 21 In : 1 Col : 1 Sel : 0 Dos\Windows ANSI I	INS

图表九 查看根证书 roottest. cer

🖹 E:\openssl\openssl-0.9.8\cnnic.cer - Notepad++		
文件 @) 编辑(E) 搜索(S) 视图(V) 格式(M) 语言(L) 设置(E) 宏(D) 运行(B) TextFX 插件(E) 窗口(M) ? X	
😑 cru	nic. cer	
1	BEGIN CERTIFICATE	
2	MIIEDzCCAvegAwIBAgIESTMAKTANBgkqhkiG9w0BAQUFADAyMQswCQYDVQQGEwJD	
3	TjEOMAwGA1UEChMFQ050SUMxEzARBgNVBAMTCkNOTklDIFJPT1QwHhcNMTAwMTI4	
4	MDMwMzIxWhcNMTcwNDE2MDUwMDQwWjA1MQswCQYDVQQGEwJDTjESMBAGA1UEChMJ	
5	QO5OSUMgU1NMMRIwEAYDVQQDEw1DTk5JQyBTU0wwggEiMAOGCSqGSIb3DQEBAQUA	
6	A4IBDwAwggEKAoIBAQCYv+6jDjZnaHUaim+UDGTPF2kC18tuhIO5wW5S/lgtcjxl	
7	8UxcmEo6ySgd41Cj9SJ4/XcpjXOKg9BdKf2loekQpR2/zaAMEds4yH/MaOrVTnlA	
8	onrg8+ZeO1Smf2pJVv1HCMyJo/UoOc4scydEHXey9EltdVoM1HfyBKhx8tgx6t6i	
9	Qt6lJ35Fi5pj5R00FCeHIOtpBcGdr85x2/bZcBhD3dopOIgAgVC/F9e8eAVf/w3j	
10	pdc++Q6QzC451E4v78JrHP9SqPRJcK35IxeC+12P4W0Pzf6poTDJ/DgYiMG0yNeK	
11	EUv/HolKk3tC9CsKwvmKPehwUwUTmwGVoFf19GcZAgMBAAGjggEoMIIBJDAfBgNV	
12	HSMEGDAWgBR18jGtKvf33VKWCscCwQ7vptU7ETAPBgNVHRMBAf8EBTADAQH/MD8G	
13	$\tt A1UdIAQ4MDYwNAYKKwYBBAGB6QwBATAmMCQGCCsGAQUFBwIBFhhodHRw018vd3d3$	
14	LmNubmljLmNuL2Nwcy8wgYIGA1UdHwR7MHkwQqBAoD6kPDA6MQswCQYDVQQGEwJD	
15	TjEOMAwGA1UEChMFQ050SUMxDDAKEgNVBAsTA2NybDENMAsGA1UEAxMEY3JsMTAz	
16	oDGgL4YtaHR0cDovL3d3dy5jbm5pYy5jbi9kb3dubG9hZC9yb290Y3JsL0NSTDEu	
17	Y3JsMAsGA1UdDwQEAwIBBjAdBgNVHQ4EFgQURQC6ihiQUcOxyve8ZTkujFaQRDAw	
18	DQYJKoZIhvcNAQEFBQADggEBAHhTAGS/SBBszQPMaPrAxxowUM4NUInFT8+BRw/m	
19	u/mynTcNuJqGKHPr4umbTWJYf/RXH2Ojg+WmWVv5EqfnyXaX3h2RgXf3hFKCNqOX	
20	fI3RXwEG90jyYa6Ii06ziC82TT8xHuuEjdjbKsUI33q3/9MAswQJmLGmnZ1MpYsF	
21	/URuWZZGSjGf/1UjcQ9xOLz1PWATKRwOW54fInLZ46dT8SqVz/AMm/a5pqMmJah3	
22	+nGCA6PoFwXwKMfmKyH9DGLY71LDekpdIL+zOQq8rsKcSF9D+U0p5+T5j4LHR8Kp	
23	jamVk/yj7EWXcZXqHXROkZaSONwQF2aVwFYY4ZeJpZNrDeM=	
24	END CERTIFICATE	
25		
I.		
Normal 1	ength : 1492 lines : 25 In : 1 Col : 1 Sel : 0 Dos\Windows ANSI INS	

图表十 查看中级根证书 cnnic.cer

注意: 在用 notepad 打开 roottes. cer 的时候可能会出现乱码,这样我们就先直接打开 roottest. cer --详细信息--复制到文本,选择 Base64 编码 X. 509,如下图:

证书导出向导 🔀
导出文件格式 可以用不同的文件格式导出证书。
选择要使用的格式:
○DER 编码二进制 X.509 (.CER)①
● Base64 编码 X.509 (.CER) (S)
◯加密消息语法标准 - PKCS #7 证书(.P7B)@)
如果可能,将所有证书包括到证书路径中 (L)
○私人信息交换 - PKCS #12 (.PFX)(P)
如果可能,将所有证书包括到证书路径中 (U)
□ 启用加强保护(要求 IE 5.0, NT 4.0 SP4 或更高版本)促)
如果导出成功,删除密钥 (2)
< 上一步 (B) 下一步 (B) > 取消

图表十一 证书导出向导(B)

下一步, 替换之前的 roottest. cer 文件即可。

复制m1.cnnic.cn.key及m1.cnnic.cn.cer文件到Nginx安装目录下的conf目录。

6. 修改配置文件

1) 修改Nginx SSL配置模块

server {

listen 443;

server_name www.domain.com;

ssl on;

ssl_certificate /etc/ssl/ml.cnnic.cer; //公钥文件(cnnic 颁发的证书)

中国互联网络信息中心 HTTP://WWW.CNNIC.CN

ssl_certificate_key /etc/ssl/ml.cnnic.key; //私钥文件

ssl_client_certificate /etc/ssl/cnnic.cer; //中级证书

ssl_session_timeout 5m;

ssl_protocols SSLv2 SSLv3 TLSv1;

ssl_ciphers ALL:!ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP;

ssl_prefer_server_ciphers on;

location / {

root html;

index index.html index.htm;

}

}

按照以上的步骤配置完成后,重新启动 nginx(如果有设置 server.key 私钥密码,这时会提示输入) 后就可以使用 https://ml.cnni.cn 来访问了。

7. 备份服务器证书

只需备份好服务器证书文件 ml. cnnic. cn. cer 私钥保存文件 ml. cnnic. cn. key 即可。