

openssl创建CA、申请证书及其给web服务颁发证书 原创

chengong1013 2016-09-24 13:55:41 博主文章分类：Web Server

©著作权

文章标签 创建 CA openssl 文章分类 其他 系统/运维 阅读量 1万

一、创建私有的CA

1) 查看openssl的配置文件:/etc/pki/tls/openssl.cnf

```
#####
[ ca ]
default_ca = CA_default # The default ca section

#####
[ CA_default ]

dir = /etc/pki/CA # Where everything is kept
certs = $dir/certs # Where the issued certs are kept
crl_dir = $dir/crl # Where the issued crl are kept
database = $dir/index.txt # database index file.
#unique_subject = no # Set to 'no' to allow creation of
# several ctificates with same subject.
new_certs_dir = $dir/newcerts # default place for new certs.

certificate = $dir/cacert.pem # The CA certificate
serial = $dir/serial # The current serial number
crlnumber = $dir/crlnumber # the current crl number
# must be commented out to leave a V1 CRL
crl = $dir/crl.pem # The current CRL
private_key = $dir/private/cakey.pem # The private key
RANDFILE = $dir/private/.rand # private random number file

x509_extensions = usr_cert # The extensions to add to the cert

# Comment out the following two lines for the "traditional"
# (and highly broken) format.
name_opt = ca_default # Subject Name options
cert_opt = ca_default # Certificate field options

# Extension copying option: use with caution.
# copy_extensions = copy
```

2) 创建所需的文件

touch /etc/pki/CA/index.txt echo 01 >/etc/pki/CA/serial

3) CA自签证书生成私钥

cd /etc/pki/CA

(umask 066;openssl genrsa -out /etc/pki/CA/private/cakey.pem 2048)

4) 生成自签名证书

openssl req -new -x509 -key /etc/pki/CA/private/cakey.pem -days 7300 -out /etc/pki/CA/cacert.pem



chengong1013

98	57.7万	0	52
原创	人气	粉丝	评论
0	2	0	124
翻译	转载	关注	收藏

+ 关注

私信

Web Server分类的近期文章

- Tomcat配置及其LNMT/LAMT/LAMT...
- HTTP499状态码 nginx下499错误及其...
- CentOS7基于虚拟用户的vsftpd
- centos7之httpd-2.4的新特性
- web服务之httpd及其新特性

近期评论

- 浅谈小白如何读懂Redis高速缓存与持... mark。
- 10分钟带你光速入门运维工具之-Puppet 哈哈，，，禁止在本博客打广告，恶意宣传...
- corosync+pacemaker高可用集群 ctrl + F@所以pacemaker独立出来之后通常...
- haproxy+varnish+amp集群实现动静分离 我做了改动，动态资源将匹配至后端的动态...
- varnish缓存实现动静分离 总结的不错哦！

近期文章

- 浅谈小白如何读懂Redis高速缓存与持...
- 品味KVM虚拟化技术部署及其虚拟磁...
- CentOS7搭建开源分布式搜索平台EL...
- 10分钟带你光速入门运维工具之-Puppet
- 深入浅出分布式文件系统MogileFS集群

-new:生成新的证书签署请求

-x509:专用CA生成自签证书

-key:生成请求时用到的私钥文件

-days n:证书的有效期

-out /path/to/somecertfile:证书的保存路径

代码演示：

```
1. [root@centos6 ~]# ls /etc/pki/CA/
2. certs crl newcerts private
3. [root@centos6 ~]# touch /etc/pki/CA/index.txt
4. [root@centos6 ~]# ll /etc/pki/CA/
5. total 16
6. drwxr-xr-x. 2 root root 4096 May  9 22:56 certs
7. drwxr-xr-x. 2 root root 4096 May  9 22:56 crl
8. -rw-r--r--. 1 root root    0 Sep 23 07:08 index.txt
9. drwxr-xr-x. 2 root root 4096 May  9 22:56 newcerts
10. drwx-----. 2 root root 4096 May  9 22:56 private
11. [root@centos6 ~]# echo 01 > /etc/pki/CA/serial
12. [root@centos6 ~]# ll /etc/pki/CA/
13. total 20
14. drwxr-xr-x. 2 root root 4096 May  9 22:56 certs
15. drwxr-xr-x. 2 root root 4096 May  9 22:56 crl
16. -rw-r--r--. 1 root root    0 Sep 23 07:08 index.txt
17. drwxr-xr-x. 2 root root 4096 May  9 22:56 newcerts
18. drwx-----. 2 root root 4096 May  9 22:56 private
19. -rw-r--r--. 1 root root    3 Sep 23 07:09 serial
20. [root@centos6 ~]# cd /etc/pki/CA
21. [root@centos6 CA]# ls
22. certs crl index.txt newcerts private serial
23. [root@centos6 CA]# (nmask 066;openssl genrsa -out private/cakey.pem 2048)
24. -bash: nmask: command not found
25. Generating RSA private key, 2048 bit long modulus
26. ....+++
27. ....+++
28. e is 65537 (0x10001)
29. [root@centos6 CA]# cd private/
30. [root@centos6 private]# cat cakey.pem
31. -----BEGIN RSA PRIVATE KEY-----
32. MIIEpAIBAACAQEAyvOMUreRADORN9F0bk08d4n/xASELSHJzW6V2K57ma/lmB7e
33. PBrOWrGCWhZR9tF8+Ewk/OCeQLukAHLgeLlte7au7uXf6RjFwi/XXemKzEUDEcO1
34. +CKTU7wio7if86rzX8xOPmP2+l4pItqqAKp7Kx9T0uAhT7gcQKkr5iU61TvS/EJf
35. xBLtwoTRIIUdYxLI7XFZe7Lm5u0iYDHIhF70TQC3s0/1lnGEsWmAZ+uOCFy6bKck
36. v6orwDu2UfjhSqkiIJBFSvZQJqh6s3kt5dN+MyAkG1wJ6daJS87FKuguLI+ISxIJ
37. Z7tXCCQqZFle5Iu1LuwRDAoieWfw0868WI+HmQIDAQABAoIBAFaVxAo0Lv9RB9E
38. RSAp43o8bdn680kwwvwd+iAPkLvot1M3GCKcZp1azfoR07bJeT+VfNJGIj4Lz9RB
39. LnNS6Nq2/br+Z6DS6MwIDSIL2SN87epORiiu15wJz915jwQuEtboGw2TKHN4aKRu
40. Fcl18l1ba+7aYFvaeHM684ukpnGz6bRYwRDrEgUvMksFvPA2dqzvP/OjEIqvvf/l
41. d+rhOQG1B18E2oQ3048PJpgPhyceKLuuFkvFGsHofI8a5hLqD3PJ4AjHuPPF/Yqz
42. ZQwxmncv+YM9nJ/s8J5PJQ+3hPkA6pbhpM1eXHSPajnnkWiMV1RkUBltkHdJGPT9
43. h4t2o2ECgYEA5z/8HvbnX1AHC8+5mK00rkBifxUyG9FVYmGOPKJwoK16eRwUQgo
```

七日热门

- [运维流程系统](#)
- [运维管理系统](#)
- [运维审计系统](#)
- [运维CMDB系统](#)
- [白话运维监控系统-1.1 运维监控系统...](#)
- [运维！运维！！](#)
- [运维发布系统详谈](#)
- [minunix 系统运维博客](#)
- [Linux运维--系统安装](#)
- [系统运维——日志处理](#)

分类列表	更多
# Linux系统基础篇	24篇
# shell编程	2篇
# Sed/AWK/grep	4篇
# Web Server	19篇
# MySQL/MariaDB	12篇

相关标签	全部
adi证书服务器	颁发证书
ca服务器	自动颁发
证书	ca证书颁发服务器
centos	openssl
自签发证书	centos申请ca证书
ftp服务器	
颁发证书	java 颁发证书
linux	ca证书颁
发机构	linux自建ca签发证书
openssl	api
签发证书	

```
44. VboVZm5mK4LCtsMzUxobSxTgsb94106U7lXrogf1cYEQkvWL7JNg8vdIMwHs75zF
45. vXnoyCF9ZoDfr0juTP94AI4Ww8GTfSo3caL+T8pnQalu5y3JvBQIRVcCgYEA4Kw1
46. 8VAGix+QYWK9h1R35cKcnZQb0eq0ChZ8XFd7leLImPCpv7t1R86mvwIvZkYMIqD3
47. btUXk8G2ezyoufntEP5KGv9QbsQS8vFDw0RSsYkwwJZBeIUv6yPdUhnIiWT6Ozwv
48. pD6hJwVSAv7m4tNTwJLH2Ebbs22Di05q/kfQFI8CgYEA4SVD0+Xx57ok0hQhKAI7
49. BLh87Vv2mGzcI9f1gwVogJfG0S0lKStPEgAFm9/6q3w5FXXBfh9Td9yejRBt1Wrg
50. J5510LC9bCALwfk9jU0ERCoL6lWCMNvbDhomUMuCaw0O6xUnpmHINUohbJ5weZ1j
51. t8jIr2jR1XUgHAZRdkN0tisCgYAF0U+13b1LEHPsVOCqMh8Hm2hQrgi/v7KNxFo8
52. KxxN1Fq0hp3Qu6is9hd0bGtR92IwXdaFXLA0JNnLfr6kOgusV0rPnbP78NwBT25v
53. cMtdSqeJcB7JNRW6vB1B1e6LXZE5MkAcv2d+GMsx8B2PnGh+Fn+C00irGY03rK1bM
54. SApMGQKBgQCaAaZzscT3KnnZEFi3e2Ir1JMxY09zCm2xR1e70m01K0BHZsoxvcA1
55. bf19tZsoD2wPcvB6j+SLhB5jdG5iJ6SCp+vx+p/XFOR1U+3V5gD/+P9I2LZfVZ+z
56. 7YvRfXzuEiZi0h4ljBb40h8Di/0ytKnBzbWs00Trj7ariZ/WfgmTDw==
57. -----END RSA PRIVATE KEY-----
58. [root@centos6 private]# ll
59. total 4
60. -rw-r--r--. 1 root root 1679 Sep 23 07:10 cakey.pem
61. [root@centos6 private]# openssl req -new -x509 -key cakey.pem -days 7300 -out ../ca
62. cert.pem
63. You are about to be asked to enter information that will be incorporated
64. into your certificate request.
65. What you are about to enter is what is called a Distinguished Name or a DN.
66. There are quite a few fields but you can leave some blank
67. For some fields there will be a default value,
68. If you enter '.', the field will be left blank.
69. -----
70. Country Name (2 letter code) [XX]:CN
71. State or Province Name (full name) []:beijing
72. Locality Name (eg, city) [Default City]:bj
73. Organization Name (eg, company) [Default Company Ltd]:chen.com
74. Organizational Unit Name (eg, section) []:alren_1
75. Common Name (eg, your name or your server's hostname) []:centos6.localdomain
76. Email Address []:alren@163.com
77. [root@centos6 private]# cd ../
78. [root@centos6 CA]# cat cacert.pem
79. -----BEGIN CERTIFICATE-----
80. MIID7zCCAtegAwIBAgIJANE0QWU3qHpeMA0GCSqGSIb3DQEBBQUAMIGMQswCQYD
81. VQQGEwJDTjEjQMA4GA1UECAwHYmVpamluZzZELMAkGA1UEBwwCYmoxETAPBgNVBAoM
82. CGNoZW4uY29tMRAwDgYDVQQLDAdhbHJlb18xMRwwGgYDVQQDBBNjZW50b3M2Lmxv
83. Y2FsZG9tYWluMRwwGgYJKoZIhvcNAQkBFg1hbHJlbkAxNjMuY29tMB4XDTE2MDky
84. MjIzMjc1MFoXDTE2MDkxNzIzMjc1MFowGgY0xCzAJBgNVBAYTAKNOMRAwDgYDVQQI
85. DAdiZWlqaW5nMQswCQYDVQQHDAJiajERMA8GA1UECgwIY2h1bi5jb20xEDA0BgNV
86. BASMB2FscmVuXzExHDAaBgNVBAMME2NlbnRvczYubG9jYXxkb21haw4xHDAaBgkq
87. hkiG9w0BCQEWDWfscmVuQDE2My5jb20wgGgEiMA0GCSqGSIb3DQEBAQUAA4IBDwAw
88. ggEKAoIBAQDK84xSt5EAM5E30XRuTTx3iF/EBIQtkEnNbpXYrnuZr+WyHt48Gs5a
89. sYJaF1H20Xz4TCT84J5Au6QAcuB4uW17tq7u5d/pGMXCL9dd6YrMRQMRw6X4IpNT
90. vCKjuJ/zqvnfzE4+Y/b6Xiki2qoAqnsrH1M64CFPuBxAoqvmJTqV09L8Q1/EEu3C
91. hNEghR1jE5jtcVl7subm46JgMciEXvRNALezT/WwCYsXaYBn644IXLspys/qivA
92. 07ZR+OFKqSgkEVK9lAmqHqzeS3l034zICQbXAnp1o1LzsUq6C4sj4hLEg1nu1dc
93. JcPkWV7ki7Uu7BEMCIj5Z/A7zrxyj4eZAgMBAAGjUDBOMB0GA1UdDgQWBQBmophw
94. H4o7o6EFDot5NMVm+rmm2TAfBgNVHSMEGDAWgBQmophwH4o7o6EFDot5NMVm+rmm
95. 2TAMBgNVHRMEBTAQAQ/MA0GCSqGSIb3DQEBBQUAA4IBAQBkZgymfLYgWOK4RPv+
96. Vz2eW+AaYncNBcot/Ju6rByEZ/Sa4nWxNBVge/0ffSDUsmkS1UdS8oYUblQU5Kq
97. pqDaQ0jbwqoMkR+YEau0Q8R+N9WtTOWew3xprRu9BvY9jTjBG5pyFp4pq0Ec0Tm3
98. YQyzv8C+0KUS2HDi13nBRet6PjYnt7zg1I2qjAuWaz70ntwFduvNDC7biX18CyJe
99. ydLnQDGot2dXWqGo/p4eDtIPxpsaH8UCz4SHDKnKZvVOg2r85Wv4F8If0puG17m
100. qhe40zy/s+F1V0lweJ3nbk2vBSETdoZViUwRz6acy0at6zn1gcMLnwjum8jcp8K
101. IOnk
102. -----END CERTIFICATE-----
103. [root@centos6 CA]# openssl x509 -in cacert.pem -noout -text
104. Certificate:
```

```
105. Data:
106.   Version: 3 (0x2)
107.   Serial Number: 15064049706582178398 (0xd10e416537a87a5e)
108.   Signature Algorithm: sha1WithRSAEncryption
109.   Issuer: C=CN, ST=beijing, L=bj, O=chen.com, OU=alren_1, CN=centos6.localdomain/emailAddress=alren@163.com
110.   Validity
111.     Not Before: Sep 22 23:17:50 2016 GMT
112.     Not After : Sep 17 23:17:50 2036 GMT
113.   Subject: C=CN, ST=beijing, L=bj, O=chen.com, OU=alren_1, CN=centos6.localdomain/emailAddress=alren@163.com
114.   Subject Public Key Info:
115.     Public Key Algorithm: rsaEncryption
116.     Public-Key: (2048 bit)
117.     Modulus:
118.       00:ca:f3:8c:52:b7:91:00:33:91:37:d1:74:6e:4d:
119.       3c:77:89:ff:c4:04:84:2d:28:49:cd:6e:95:d8:ae:
120.       7b:99:af:e5:98:1e:de:3c:1a:ce:5a:b1:82:5a:16:
121.       51:f6:d1:7c:f8:4c:24:fc:e0:9e:40:bb:a4:00:72:
122.       e0:78:b9:6d:7b:b6:ae:ee:e5:df:e9:18:c5:c2:2f:
123.       d7:5d:e9:8a:cc:45:03:11:c3:a5:f8:22:93:53:bc:
124.       22:a3:b8:9f:f3:aa:f3:5f:cc:4e:3e:63:f6:fa:5e:
125.       29:22:da:aa:00:aa:7b:2b:1f:53:3a:e0:21:4f:b8:
126.       1c:40:a2:ab:e6:25:3a:95:3b:d2:fc:42:5f:c4:12:
127.       ed:c2:84:d1:20:85:1d:63:12:c8:ed:71:59:7b:b2:
128.       e6:e6:e3:a2:60:31:c8:84:5e:f4:4d:00:b7:b3:4f:
129.       f5:96:71:84:b1:69:80:67:eb:8e:08:5c:ba:6c:a7:
130.       24:bf:aa:2b:c0:3b:b6:51:f8:e1:4a:a9:22:20:90:
131.       45:4a:f6:50:26:a8:7a:b3:79:2d:e5:d3:7e:33:20:
132.       24:1b:5c:09:e9:d6:89:4b:ce:c5:2a:e8:2e:2c:8f:
133.       88:4b:12:09:67:bb:57:5c:24:2a:64:59:5e:e4:8b:
134.       b5:2e:ec:11:0c:0a:22:79:67:f0:3b:ce:bc:58:8f:
135.       87:99
136.     Exponent: 65537 (0x10001)
137.   X509v3 extensions:
138.     X509v3 Subject Key Identifier:
139.       26:A2:98:70:1F:8A:3B:A3:A1:05:0E:8B:79:34:C5:66:FA:B9:A6:D9
140.     X509v3 Authority Key Identifier:
141.       keyid:26:A2:98:70:1F:8A:3B:A3:A1:05:0E:8B:79:34:C5:66:FA:B9:A6:D9
142.     X509v3 Basic Constraints:
143.       CA:TRUE
144.   Signature Algorithm: sha1WithRSAEncryption
145.     64:66:0c:a6:7c:b6:20:58:e2:b8:44:fb:fe:57:3b:36:79:6f:
146.     80:69:83:5c:34:17:28:b7:f2:6e:ea:b0:72:11:9f:d2:6b:89:
147.     d6:c4:d0:55:81:ef:f4:7d:f4:83:52:c9:a4:4a:55:1d:4b:ca:
148.     18:51:b2:d0:53:92:aa:a6:a0:da:43:48:db:c2:aa:0c:91:1f:
149.     98:11:ab:b4:43:c4:7e:37:d5:ad:4c:e5:9e:c3:7c:69:ad:1b:
150.     bd:06:f6:3d:8d:38:c1:1b:9a:72:16:9e:29:a8:e1:1c:39:39:
151.     b7:61:0c:b3:bf:c0:be:d0:a5:12:d8:70:e2:d7:79:c1:45:eb:
152.     7a:3e:36:27:b7:bc:e0:88:8d:aa:8c:0b:96:6b:3e:f4:9e:dc:
153.     05:76:eb:cd:0c:2e:db:89:7d:7c:0b:22:5e:c9:d2:e7:40:31:
154.     a8:b7:67:57:5a:a1:a8:fe:9e:1e:0e:d2:0f:c6:9b:1a:1f:c5:
155.     02:cf:84:87:0c:a9:ca:66:f5:4e:83:6a:fc:e5:6b:f8:17:c2:
156.     1f:d2:9b:86:1a:5e:e6:aa:17:b8:d3:3c:bf:b3:e1:75:57:49:
157.     56:78:9d:e7:6e:4d:af:05:21:13:76:86:55:89:45:ae:47:3e:
158.     9a:73:2d:1a:b7:ac:e7:96:07:0c:2e:7c:23:ba:6f:23:72:9f:
159.     0a:20:e9:ca
160. [root@centos6 CA]# openssl x509 -in cacert.pem -noout -dates
161. notBefore=Sep 22 23:17:50 2016 GMT
162. notAfter=Sep 17 23:17:50 2036 GMT
```

二、颁发及其吊销证书

1)颁发证书, 在需要使用证书的主机生成证书请求, 给web服务器生成私钥(本实验在另一台主机上)

```
(umask 066;openssl genrsa -out /etc/httpd/ssl/httpd.key 2048)
```

2)生成证书申请文件

```
openssl req -new-key /etc/httpd/ssl/httpd.key -days 365 -out /etc/httpd/ssl/httpd.csr
```

3)将证书文件传给CA, CA签署证书并将证书颁发给请求者,注意:默认国家、省和公司必须和CA一致

```
openssl ca -in /tmp/httpd.csr -out /etc/pki/CA/certs/httpd.crt -days 365
```

4)查看证书中的信息

```
opessl x509 -in /path/from/cert_file -noout -text|subject|serial|dates
```

5)吊销证书, 在客户端获取要吊销的证书的serial

```
openssl x509 -in /PATH/FROM/CERT_FILE -noout -serial -subject
```

6)在CA上, 根据客户提交的serial与subject信息, 对比检验 是否与index.txt文件中的信息一致吊销证书

```
openssl ca -revoke /etc/pki/CA/newcerts/ SERIAL.pem
```

7)生成吊销证书的编号(第一次吊销一个证书时才需要执行)

```
echo 01 > /etc/pki/CA/crlnumber
```

8)更新证书吊销列表, 查看crl文件

```
openssl ca -gencrl -out /etc/pki/CA/crl/ca.crl
```

```
openssl crl -in /etc/pki/CA/crl/ca.crl -noout -text
```

9)安装mod_ssl模块并修改/etc/httpd/conf.d/ssl.conf配置文件

```
DocumentRoot "/web/pma"
```

```
ServerName www.chen.net:443
```

```
<Directory "/web/pma">
```

```
AllowOverride All
```

```
Options None
```

```
require all granted
```

```
</Directory>
```

```
SSLCertificateFile /etc/httpd/ssl/httpd.crt
```

图示：

授权目录

```
# General setup for the virtual host, inherited from global configuration
DocumentRoot "/web/pma"
ServerName www.chen.net:443
<Directory "/web/pma">
    AllowOverride All
    Options None
    require all granted
</Directory>

# Use separate log files for the SSL virtual host; note that LogLevel
# is not inherited from httpd.conf.
ErrorLog logs/ssl_error_log
TransferLog logs/ssl_access_log
LogLevel warn

#    SSL Engine Switch:
#    Enable/Disable SSL for this virtual host.
SSLEngine on

#    SSL Protocol support:
# List the enable protocol levels with which clients will be able to
"/etc/httpd/conf.d/ssl.conf" 223L, 9508C          62,3          23%
```

```
#    Server Certificate:
# Point SSLCertificateFile at a PEM encoded certificate.  If
# the certificate is encrypted, then you will be prompted for a
# pass phrase.  Note that a kill -HUP will prompt again.  A new
# certificate can be generated using the genkey(1) command.
SSLCertificateFile /etc/httpd/ssl/httpd.crt

#    Server Private Key:
# If the key is not combined with the certificate, use this
# directive to point at the key file.  Keep in mind that if
# you've both a RSA and a DSA private key you can configure
# both in parallel (to also allow the use of DSA ciphers, etc.)
SSLCertificateKeyFile /etc/httpd/ssl/httpd.key

#    Server Certificate Chain:
# Point SSLCertificateChainFile at a file containing the
# concatenation of PEM encoded CA certificates which form the
# certificate chain for the server certificate.  Alternatively
# the referenced file can be the same as SSLCertificateFile
# when the CA certificates are directly appended to the server
# certificate for convinience.
#SSLCertificateChainFile /etc/pki/tls/certs/server-chain.crt
```

10)测试

openssl s_client [-connect host:port] [-cert filename] [-CApath directory] [-CAfile filename]

实例：

openssl s_client -connect www.chen.net:443 -CAfile /etc/pki/CA/cacert.pem

curl --cacert /etc/pki/CA/cacert.pem https://www.chen.net/

实现图示：




欢迎使用 phpMyAdmin

语言 - *Language*

中文 - Chinese simplified ▼

登录

用户名:

密码:

执行

代码演示：

```
1. [root@chen ~]# {umask 066;openssl genrsa -out /etc/pki/tls/private/httpd.key 2048}
2. Generating RSA private key, 2048 bit long modulus
3. ....+++
4. ....+++
5. e is 65537 (0x10001)
6. [root@chen ~]# cd /etc/pki/tls/private/
7. [root@chen private]# cat httpd.key
8. -----BEGIN RSA PRIVATE KEY-----
9. MIIEpAIBAAKCAQEAYdNdaHEea6lQpeMOof1bARNbNjerS+CG6bZWxYp3FVIEsqnQ
10. 5dGZ9uvWfCn3XWAb3nTQR0cEjULIkLQS/RnoQA3t9uy83+PmL7imXnB6eDhBX0hb
11. QYXjAyShhR/Y+OHBjT6HhDZYxqNPoKIxi70bJVmG6ovuE8P5SQQJ15bX21/YB+CmJ
12. PpoY37WVd4lJagECSK2NjIuMcdMnmIKZIZgCU3XKw1kDsG8DJXj7ZVuiimgspM
13. wyXFI94vHdVxQ7mEJiIBT3F9rn95+Fy35p+fHBcXS4Iw+gJaa4GZeOuYaNxdwI9l
14. 9nLwx9hW69UJ0wcuJQGc8kyN8AFu1/sh2aWExQIDAQABAoIBAQC4snRN6w9CyVzj
15. oqm2dsV8bQFQ2ZsqQhXU7yFzeWbHHRrtgdiJKMq0nFh77Dh1PFnkt5QPVP+EwrQX
16. MKQb+cSAMf8utLGYVtBFpb6iuF5rFFctUs16Ge6baBe2q10AhMmiVWtGasehT+O
17. qj+bME9v28FLDa1fbz3HoaksdyG/ptb6MEh/8Z4bAFovyYfI+IY+P3dzDd018Sv
18. V6wgj+A11wmhNUyete++DoO/JJtQJZuh0LeN4eg2W51M9vnnH7hrosyRwHfcYioU
19. SUoKEws4Md78zVL7IEFcRwV3mSgm356u9SK12gs+X9Qpb9Uyt5zs1q2jxGxwoe5s
20. ige9ERbVAoGBAPBIOELs4Cvdr1McaYbvnU6XfCVuWti0ZFDKcEak2XUz2xMaCeBV
21. WPFnHq0PiC52RG8h0f9cqSt6m3rB8/5HjTuf9fyv2C6rnpUxfzqZ0P3euMBPIMHM
22. e2nBwr6hOMNeQwxs6YfXILlCRzMub4c4jqxNGESrWoQTogFe4TEINoe/AoGBANCG
23. yXsZRwI76lPEm5Z8eyFiHqKAq+QazyZoH1xXW6ByqtDA6toqHG0tuzhUIwR2HfiG
24. O2I3CWYVnIxWcnBMvdJ4XwIORVzfG9sh6fBqCRbYd2LhD6xTXPqq6dfssT/qI2q1
25. Cy5PNc0Q2XDFdar0dpIbjcYuxGP1PP1DtdwALR7AoGBAJtZKRvrAHn72nVuYh+W
```

```
26. XWrJb783iM6gw1cNeudwr8UhoJrJ8+aw51NWrcp11irPf9iMjOcKXu1P6jLV
27. Cc+pzLzw52DNHjsxBCpb/I2V6HaU8gw58XRfjEv5KhznNawZ6IwInweYTIQfmoWf
28. IEbv1SgYb04FT3F5aThtKew7AoGADojo6adFw4L1ThBGLB/x+sm1JGrqM5sUUZZM
29. OG03T9swbLF9qA2cqag+tYoKa+zIDdQU/QiXXA0t7daSGcE2O5njYjIwwhat69N
30. LvEb+C1dtJNeCdoAuPkAoZXgTV+4USci4Fh+XIQ9DoBqecnYkfXPI05NBtzbxri/
31. DhUGFy0CgYB6Q0T2w3e8SkGf6FSgqIe4u5vio6RCsPIVhHuuZacOgeyzAqCEwQJg
32. b3SDZIxAUyPAnhNtk1lnAYSKdFa97fXyGudLNh0otj74C9Na6yLrUQ8zdEC1o3u
33. VOJy0057bfBykghXYi9JN+29sBB0Y0j9uDE0nOUIr95eiwKsP5QXg==
34. -----END RSA PRIVATE KEY-----
35. [root@chen private]# openssl req -new -key /etc/pki/tls/private/httpd.key -days 365 -out httpd.csr
36. You are about to be asked to enter information that will be incorporated
37. into your certificate request.
38. What you are about to enter is what is called a Distinguished Name or a DN.
39. There are quite a few fields but you can leave some blank
40. For some fields there will be a default value,
41. If you enter '.', the field will be left blank.
42. -----
43. Country Name (2 letter code) [XX]:CN
44. State or Province Name (full name) []:beijing
45. Locality Name (eg, city) [Default City]:bj
46. Organization Name (eg, company) [Default Company Ltd]:chen.com
47. Organizational Unit Name (eg, section) []:alren_1
48. Common Name (eg, your name or your server's hostname) []:www.alren.com
49. Email Address []:admin@chen.com
50. Please enter the following 'extra' attributes
51. to be sent with your certificate request
52. A challenge password []:
53. An optional company name []:
54. [root@chen private]# ls
55. httpd.csr httpd.key
56. [root@chen private]# scp httpd.csr 10.1.249.94:
57. [root@centos6 CA]# cp /root/httpd.csr .
58. [root@centos6 CA]# ls
59. cacert.pem certs crl httpd.csr index.txt newcerts private serial
60. [root@centos6 CA]# openssl ca -in httpd.csr -out certs/httpd.crt
61. Using configuration from /etc/pki/tls/openssl.cnf
62. Check that the request matches the signature
63. Signature ok
64. Certificate Details:
65.     Serial Number: 1 (0x1)
66.     Validity
67.         Not Before: Sep 22 23:43:02 2016 GMT
68.         Not After : Sep 22 23:43:02 2017 GMT
69.     Subject:
70.         countryName           = CN
71.         stateOrProvinceName   = beijing
72.         organizationName      = chen.com
73.         organizationalUnitName = alren_1
74.         commonName            = www.alren.com
75.         emailAddress          = admin@chen.com
76.     X509v3 extensions:
77.         X509v3 Basic Constraints:
78.             CA:FALSE
79.         Netscape Comment:
80.             OpenSSL Generated Certificate
81.         X509v3 Subject Key Identifier:
82.             CA:82:B2:CF:4A:A2:49:9B:1D:46:84:04:F8:C6:F6:0D:E0:49:B7:A4
83.         X509v3 Authority Key Identifier:
84.             keyid:26:A2:98:70:1F:8A:3B:A3:A1:05:0E:8B:79:34:C5:66:FA:B9:A6:D9
85.
86. Certificate is to be certified until Sep 22 23:43:02 2017 GMT (365 days)
```



```
87. Sign the certificate? [y/n]:y
88.
89. 1 out of 1 certificate requests certified, commit? [y/n]y
90. Write out database with 1 new entries
91. Data Base Updated
92. [root@centos6 CA]# ls
93. cacert.pem  crl      index.txt      index.txt.old  private  serial.old
94. certs       httpd.csr  index.txt.attr newcerts       serial
95. [root@centos6 CA]# cat index.txt.attr
96. unique_subject = yes
97. [root@centos6 CA]# cat index.txt
98. V 170922234302Z 01 unknown / C=CN/ST=beijing/O=chen.com/OU=alren_1/CN=www.alren.com/emailAddress=admin@chen.com
99. [root@centos6 CA]# cat serial
100. 02
101. [root@centos6 CA]# cd certs/
102. [root@centos6 certs]# ls
103. httpd.crt
104. [root@centos6 certs]# openssl x509 -in httpd.crt -noout -text
105. Certificate:
106.     Data:
107.         Version: 3 (0x2)
108.         Serial Number: 1 (0x1)
109.         Signature Algorithm: sha1WithRSAEncryption
110.         Issuer: C=CN, ST=beijing, L=bj, O=chen.com, OU=alren_1, CN=centos6.localdomain/emailAddress=alren@163.com
111.         Validity
112.             Not Before: Sep 22 23:43:02 2016 GMT
113.             Not After : Sep 22 23:43:02 2017 GMT
114.         Subject: C=CN, ST=beijing, O=chen.com, OU=alren_1, CN=www.alren.com/emailAddress=admin@chen.com
115.         Subject Public Key Info:
116.             Public Key Algorithm: rsaEncryption
117.             Public-Key: (2048 bit)
118.             Modulus:
119.                 00:c9:d3:5d:68:71:1e:6b:a9:50:a5:e3:0e:a1:fd:
120.                 5b:01:13:5b:36:37:ab:4b:e0:86:e9:b6:56:c5:8a:
121.                 77:15:52:04:b2:a9:d0:e5:d1:99:f6:eb:d6:15:c3:
122.                 77:5d:60:1b:de:74:d0:47:47:04:8d:42:c8:90:b4:
123.                 12:fd:19:e8:40:0d:ed:f6:ec:bc:df:e3:e6:2f:b8:
124.                 a6:5e:70:7a:78:38:41:5c:e8:5b:41:85:e3:03:24:
125.                 a1:85:1f:d8:f8:e1:c1:25:3e:87:84:36:58:c6:a3:
126.                 4f:a0:a2:31:8b:b3:9b:25:59:86:ea:8b:ee:13:c3:
127.                 f9:49:02:65:e5:b5:f6:d7:f6:01:f8:29:89:3e:9a:
128.                 18:df:b5:95:77:89:49:6a:01:02:48:ad:8d:8c:8b:
129.                 8c:09:d3:27:98:82:99:21:98:02:53:75:ca:9f:0d:
130.                 64:0e:c1:bc:0c:95:e3:ed:95:6e:8a:29:b1:82:ca:
131.                 4c:c3:25:c5:23:de:2f:1c:35:71:43:b9:84:26:22:
132.                 01:4f:71:7d:ae:7f:79:f8:5c:b7:e6:9f:9f:1c:17:
133.                 17:4b:82:30:fa:02:5a:6b:81:99:78:eb:98:68:dc:
134.                 5d:c0:8f:65:f6:72:f0:c7:d8:56:eb:d5:09:d3:07:
135.                 2e:25:01:9c:f2:4c:8d:f0:01:6e:97:fb:21:d9:a5:
136.                 84:c5
137.             Exponent: 65537 (0x10001)
138.         X509v3 extensions:
139.             X509v3 Basic Constraints:
140.                 CA:FALSE
141.             Netscape Comment:
142.                 OpenSSL Generated Certificate
143.             X509v3 Subject Key Identifier:
144.                 CA:82:B2:CF:4A:A2:49:9B:1D:46:84:04:F8:C6:F6:0D:E0:49:B7:A4
145.             X509v3 Authority Key Identifier:
146.                 keyid:26:A2:98:70:1F:8A:3B:A3:A1:05:0E:8B:79:34:C5:66:FA:B9:A6:D9
147.
```

```
148.      Signature Algorithm: sha1WithRSAEncryption
149.      5f:b8:37:e2:e5:e0:5e:65:99:60:9f:2f:5a:81:7e:55:e7:dc:
150.      85:94:bc:d0:ae:82:db:c0:cd:bb:0c:7c:7d:6e:97:41:35:94:
151.      71:d9:bc:a4:3e:76:d1:4e:09:3d:a2:a9:5e:a2:24:9c:98:f3:
152.      ac:7d:ea:f0:f2:ff:17:0d:47:fb:47:04:d6:29:7f:d8:3a:08:
153.      df:33:45:8c:15:2a:a0:be:03:dc:4e:9c:91:ef:a1:99:a8:6d:
154.      f2:4c:10:1d:9c:7b:23:28:0a:17:bd:cf:c4:2d:c6:07:d1:73:
155.      48:2c:f9:a0:0f:2a:21:d0:f7:a4:9c:85:d5:75:02:c0:09:19:
156.      97:b8:aa:1d:e0:e3:8a:39:29:f5:4c:d7:69:01:e8:e6:50:91:
157.      fe:75:8a:3d:75:1c:df:94:36:01:32:43:4e:9c:49:f4:4c:f2:
158.      d9:85:9d:45:89:7f:6d:47:a9:48:48:bc:b3:8b:ed:06:34:f5:
159.      30:6e:c9:8f:a9:54:f6:6d:e7:2d:ce:03:9d:2f:ea:fa:47:fa:
160.      ee:13:f2:26:3b:a8:7a:e8:fd:66:ae:c6:97:37:03:a7:e8:c7:
161.      ad:c3:d9:e1:b1:b9:b0:61:ba:34:ea:80:6b:42:e4:d9:b7:38:
162.      0d:49:13:b1:89:2f:ca:a0:aa:69:e5:95:c0:c0:e3:ba:af:9f:
163.      68:80:5a:4f
164. [root@centos6 certs]#
165. [root@centos6 certs]#
166. [root@centos6 certs]# openssl ca -revoke httpd.crt
167. Using configuration from /etc/pki/tls/openssl.cnf
168. Revoking Certificate 01.
169. Data Base Updated
170. [root@centos6 certs]# cd ../
171. [root@centos6 CA]# ls
172. cacert.pem  crl          index.txt      index.txt.attr.old  newcerts  serial
173. certs       httpd.csr    index.txt.attr index.txt.old       private   serial.old
174. [root@centos6 CA]# cat index.txt
175. R 170922234302Z 160922234706Z 01 unknown /C=CN/ST=beijing/O=chen.com/OU=alren_1/CN=www.alren.com/emailAddress=admin@chen.com
176. [root@centos6 CA]# echo 01 > crlnumber
177. [root@centos6 CA]# openssl ca -gencrl -out crl
178. crl/          crlnumber
179. [root@centos6 CA]# openssl ca -gencrl -out crl/ca.crl
180. Using configuration from /etc/pki/tls/openssl.cnf
181. [root@centos6 CA]# cat crl/ca.crl
182. -----BEGIN X509 CRL-----
183. MIIB/TCB5gIBATANBgkqhkiG9w0BAQUFADCbjTElMAkGA1UEBhMCQ04xEDA0BgNV
184. BAGMB2JlaWppbmxcCzAJBgNVBAMAMjQmREwYDVQQKDAhjaGVuLmNvbTEQMA4G
185. A1UECwwHYWxyZW5fMTEcMBoGA1UEAwTY2VudG9zNi5sb2NhbGRvbWVfbjEjEjEz
186. CSqGSIB3DQEJARYNYWxyZW5AMTYzLmNvbRcNMTYwOTIyMjM1MDU0WhcNMTYxMDIy
187. MjM1MDU0WjAUMBICAQEXDTE2MDkyMjIzNDcwNlqgDjAMMAoGA1UdFAQDAgEBMA0G
188. CSqGSIB3DQEBBQUAA4IBAQAQDo6PBGbyqpM+noDuaDZxy349jgqcmRLCPDYKRZ4L+
189. 1PyRTVhuIZztSUu2u5x7ZEYx3jyR7rFY8tpHRYT4ZnJe9o14pTUb8INNxo1IZ4r1
190. hG1KWKQSDS3WVrQnCswBhWcAccd9wU2+YTj4m7f1drTbu6d5elfaZR1yKsTLnZdV
191. ESKmr4MXjcd0F80Q8Dc0hpkVKt71JiDwJt0WuHI6XPz90ta8EAN7Ry87Ajf9/HD
192. LDnOWEEA50F7JgUQgFKI72wvekQoZ9Cj/KeFb0ov+wde7+uCGNqRcPLznnTxvZ8a
193. e0/e9HGQaDLGKDoN/vxVXCRQ030fZrPzag810yqSxxgZ
194. -----END X509 CRL-----
195. [root@centos6 CA]# openssl crl -in crl/ca.crl -noout -text
196. Certificate Revocation List (CRL):
197.      Version 2 (0x1)
198.      Signature Algorithm: sha1WithRSAEncryption
199.      Issuer: /C=CN/ST=beijing/L=bj/O=chen.com/OU=alren_1/CN=centos6.localdomain/emailAddress=alren@163.com
200.      Last Update: Sep 22 23:50:54 2016 GMT
201.      Next Update: Oct 22 23:50:54 2016 GMT
202.      CRL extensions:
203.          X509v3 CRL Number:
204.              1
205. Revoked Certificates:
206.      Serial Number: 01
207.      Revocation Date: Sep 22 23:47:06 2016 GMT
208.      Signature Algorithm: sha1WithRSAEncryption
```

```
209.      03:a3:a3:c1:19:bc:aa:a4:cf:a7:a0:3b:9a:0d:9c:72:df:8f:
210.      63:82:a7:26:44:b0:8f:0d:82:91:67:82:fe:d4:fc:91:4d:58:
211.      6e:21:9c:ed:49:4b:b6:bb:9c:7b:64:46:31:de:3c:91:ee:b1:
212.      58:f2:da:47:45:84:f8:66:72:5e:f6:89:78:a5:35:1b:f0:83:
213.      4d:c7:49:48:67:8a:f5:84:69:4a:58:a4:12:0d:2d:d6:56:b4:
214.      27:0a:cc:01:85:67:00:71:c7:7d:c1:4d:be:61:38:f8:9b:b7:
215.      f5:76:b4:db:bb:a7:79:7a:57:da:65:1d:72:2a:c4:cb:9d:97:
216.      55:11:22:a6:af:83:17:8d:c0:f4:17:cd:10:f0:37:34:86:92:
217.      95:2a:de:f5:26:20:f0:26:dd:16:b8:72:3a:5c:fc:fd:d2:d6:
218.      bc:10:03:7b:47:2f:3b:02:3f:1f:f7:f1:c3:2c:39:ce:58:41:
219.      00:e7:41:7b:26:05:10:80:52:88:ef:6c:2f:7a:44:28:67:d0:
220.      a3:fc:a7:85:6c:ea:2f:fb:07:5e:ef:eb:82:18:da:91:70:f2:
221.      f3:9e:74:f1:57:3f:1a:7b:4f:de:f4:71:90:68:32:c6:28:3a:
222.      0d:fe:fc:55:5c:24:50:d3:7d:1f:66:b3:f3:6a:0f:35:d3:2a:
223.      92:c7:18:19
224. [root@centos6 CA]#
```

不同主机之间拷贝文件小技巧：

在使用ssh远程登录时提示:remote host indentification has changed!则需清除~/.ssh/known_hosts文件即可，因为系统检测出rsa钥匙发生了改变。清除此配置文件重连。

```
1. [root@centos6 ~]# ssh 10.1.229.40
2. @@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
3. @      WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!      @
4. @@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
5. IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
6. Someone could be eavesdropping on you right now (man-in-the-middle attack)!
7. It is also possible that the RSA host key has just been changed.
8. The fingerprint for the RSA key sent by the remote host is
9. 3d:bb:7b:99:51:b3:9f:b8:81:4e:fd:6e:b5:ac:92:02.
10. Please contact your system administrator.
11. Add correct host key in /root/.ssh/known_hosts to get rid of this message.
12. Offending key in /root/.ssh/known_hosts:1
13. RSA host key for 10.1.229.40 has changed and you have requested strict checking.
14. Host key verification failed.
15.
16. [root@centos6 .ssh]#
17. [root@centos6 .ssh]# ssh root@10.1.229.93
18. The authenticity of host '10.1.249.93 (10.1.249.93)' can't be established.
19. RSA key fingerprint is d3:e3:99:1d:b6:00:fe:18:26:58:a5:7d:eb:14:c3:57.
20. Are you sure you want to continue connecting (yes/no)? yes
21. Warning: Permanently added '10.1.229.93' (RSA) to the list of known hosts.
22. root@10.1.249.93's password:
```



2赞



2收藏



评论



分享

上一篇：忘记mysql数据库密码怎么办？

下一篇：web服务之httpd虚拟主机配置你造吗？



提问和评论都可以，用心的回复会被更多人看到

评论

相关文章

创建CA颁发证书

证书 一、建立CA服务器 修改配置文件 # vim /etc/pki/tls/openssl.cnf ##### [CA_default] dir = /etc...

CA如何自签证书及颁发证书？

证书 1.CA自签证书 cd /etc...

使用openssl给web站点颁发证书

背景介绍在生产环境中，有时需要用到自签名的证书，而谷歌浏览器从2016年开始就降低了sha1的算法级别，openssl默认使用的是sha1的算法，以下就来介绍openssl如何...



OpenSSL架设私有CA颁发证书

一、安装openssl二、openssl常用命令、选项三、证书申请、自建CA、颁发证书 一、opensslopenssl是一个强大的安全套接字层密码库，囊括主要的密码算法、常用的密钥和证书封装管理...

ca 颁发证书

ca 颁发证书

使用OpenSSL 自建CA 以及颁发证书

一个自己写的CA证书创建脚本，写之前以为这是一个简单的脚本，当开始写后才发现这是个坑#!/bin/bash #####...



创建私有CA及颁发证书

证书申请及签署步骤：1、生成**申请**请求 2、RA核验 3、**CA**签署 4、获取**证书**三种策略：匹配、支持和可选 ①匹配:指要求**申请**填写的信息跟**CA**设置信息必须一致，默认国...



创建CA自签证书及发证

创建所需要的文件。cd /etc/pki/**CA**目录中，在此目录中 touch index.txt文件echo 01 > serial**CA**自签**证书** (umask 077;**openssl** genrsa -out private/cakey.pem 2048) 这一步是建立私钥，**ope...**

CA自签名证书，并给服务器颁发证书

https **CA**自签名**证书**，并给Webserver颁发**证书** `` # ****CA**主机执行命令** [root@centos7 ~]# cd /etc/pki/**CA** [root@centos7 **CA**]# touch index.txt [root@centos7 **CA**]# echo 01 > serial 生成...

脚本实现创建CA并颁发证书

#!/bin/bashchopenssl() {MYOPENSSL=/etc/pki/tls/**openssl**.cnf sed -i 's@../**CA**@/etc/pki/**CA**@g' \$MYOPENSSL sed -i 's@= GB@= CN@g' \$MYOPENSSL sed -i 's@= Berkshire@= Henan...

linux下创建CA以及颁发证书

一、创建私有**CA**：使用工具**openssl**模拟创建CA**openssl**程序包分解:**Openssl**由三部分组成：加密库libcrypt、**服务器**端实现ssl功能会话的库、命令行工具**Openssl**工具使用详解...



Linux建立私有CA和颁发证书及管理

建立私有**CA**和颁发**证书**及管理 ## 1. 建立私有**CA** 1. 使用**openssl**工具实现搭建一个私有**CA**，打开文件*/etc/pki/tls/**openssl**.cnf*，文件里的内容是***openssl*** 的配置文件。 - 三种策略：matc...

自签证书和申请颁发证书

做一个自签**证书**过程 1 进入/etc/pki/**CA**/private 生成一个密钥文件 [root@station40 certs]# cd /etc/pki/**CA**/private/ [root@station40 private]# ls my.key [root@station40 private]# **openssl** g...

Openssl 创建CA和申请证书

Openssl 创建**CA**和**申请证书**=====概述： 本章是上篇加密解密技术的续，主要...



使用OpenSSL颁发CA证书

使用**OpenSSL**颁发**CA**证书 **CA**服务器端 使用cd 切换到/etc/pki/**CA** 在**CA**下使用命令(umask 66; **openssl** genrsa 2048 > private/cakey.pem)生成**CA**证书的私钥；使用命令 ll pr...



Linux创建私有CA证书及证书颁布（即用openssl生成ca证书）

最近碰到个需要用nginx proxy做https代理的情况，需要在代理机上搭一个nginx proxy，此时就需要用到自建**证书**，于是有了这一篇文章，记录一下，持续更新中，敬请期待 ...

CA是如何颁发证书的

&n...

使用OpenSSL创建CA和申请证书

OpenSSL简介 **OpenSSL**是一种加密工具套件，可实现安全套接字层（SSL v2 / v3）和传输层安全性（TLS v1）网络协议以及它们所需的相关加密标准。**openssl**命令行工具用于从shell...

openssl加密解密及CA自签颁发证书详解

原文地址：http://tanxw.blog.51cto.com/4309543/1379417前言 **openssl**是一款功能强大的加密工具、我们当中许多人已经在使用**openssl**、用于创建RSA私钥或**证书**签名请...



返回顶部

