Table Of Contents

nixCraft: Linux Tips, Hacks, Tutorials, And Ideas In Blog Format
http://www.cyberciti.biz/

How To Verify SSL Certificate From A Shell Prompt

Posted by Vivek Gite <vivek@nixcraft.com>


[1]

How do I verify and diagnosis SSL certification installation from a Linux / UNIX shell prompt? How do I validate SSL Certificate installation and save hours of troubleshooting headaches without using a browser? How do I confirm I've the correct and working SSL certificates?

OpenSSL comes with a generic SSL/TLS client which can establish a transparent connection to a remote server speaking SSL/TLS. It's intended for testing purposes only and provides only rudimentary interface functionality but internally uses mostly all functionality of the OpenSSL ssl library. For testing purpose I will use mail.nixcraft.net:443 [2] SSL certificate which is issued by Go Daddy.

Step # 1: Getting The Certificate

Create directory to store certificate:

```
$ mkdir -p ~/.cert/mail.nixcraft.net/
$ cd ~/.cert/mail.nixcraft.net/
```

Retrieve the mail.nixcraft.net certificate provided by the nixcraft HTTPD mail server:

```
$ openssl s_client -showcerts -connect mail.nixcraft.net:443
```

Sample output:

```
CONNECTED(00000003)
depth=0 /O=mail.nixcraft.net/CN=mail.nixcraft.net/OU=Domain Control Validated
verify error:num=20:unable to get local issuer certificate
verify return:1
depth=0 /O=mail.nixcraft.net/CN=mail.nixcraft.net/OU=Domain Control Validated
verify error:num=27:certificate not trusted
verify return:1
depth=0 /O=mail.nixcraft.net/CN=mail.nixcraft.net/OU=Domain Control Validated
verify error:num=21:unable to verify the first certificate
verify return:1
---
Certificate chain
 0 s:/O=mail.nixcraft.net/CN=mail.nixcraft.net/OU=Domain Control Validated
   i:/C=US/ST=Arizona/L=Scottsdale/O=GoDaddy.com, Inc./OU=http://certificates.godaddy.com/r
-----BEGIN CERTIFICATE-----
MIIE5zCCA8+gAwIBAgIEAOJk2zANBgkqhkiG9w0BAQUFADCByjELMAkGA1UEBhMC
VVMxEDAOBgNVBAgTB0FyaXpvbmExEzARBgNVBAcTClNjb3R0c2RhbGUxGjAYBgNV
BAoTEUdvRGFkZHkuY29tLCBJbmMuMTMwMQYDVQQLEypodHRwOi8vY2VydGlmaWNh
dGVzLmdvZGFkZHkuY29tL3J1cG9zaXRvcnkxMDAuBgNVBAMTJ0dvIERhZGR5IFNl
Y3VyZSBDZXJ0aWZpY2F0aW9uIEF1dGhvcml0eTERMA8GA1UEBRMIMDc5NjkyODcw
HhcNMDkwMTE4MjEyMjMxWhcNMTEwMTE4MjEyMjMxWjBbMRowGAYDVQQKExFtYWls
Lm5peGNyYWZ0Lm5ldDEaMBgGA1UEAxMRbWFpbC5uaXhjcmFmdC5uZXQxITAfBgNV
BAsTGERvbWFpbiBDb250cm9sIFZhbGlkYXRlZDCBnzANBgkqhkiG9w0BAQEFAAOB
jQAwgYkCgYEA0LhCDXvNXhTHov9Szh474Cv3Nz7QspVOI4p5M+zZt18VTVCHJz0Z
TleJum8RblpU4NPHJgOauIb1CAE3vLSKySV2DjHMt2L2/NUatJiKjDQKAEloKwQK
t75BP0mAGFPZmHlMNUQ32Sr/0byxxM4ElL2SSBasJE3PPVkSBOtLfssCAwEAAaOC
AcUwggHBMA8GA1UdEwEB/wQFMAMBAQAwHQYDVR0lBBYwFAYIKwYBBQUHAwEGCCsG
AQUFBwMCMA4GA1UdDwEB/wQEAwIFoDAyBgNVHR8EKzApMCegJaAjhiFodHRwOi8v
Y3JsLmdvZGFkZHkuY29tL2dkczEtMS5jcmwwUwYDVR0gBEwwSjBIBgtghkgBhv1t
AQcXATA5MDcGCCsGAQUFBwIBFitodHRwOi8vY2VydGlmaWNhdGVzLmdvZGFkZHku
Y29tL3JlcG9zaXRvcnkvMIGABggrBgEFBQcBAQR0MHIwJAYIKwYBBQUHMAGGGGh0
dHA6Ly9vY3NwLmdvZGFkZHkuY29tLzBKBggrBgEFBQcwAoY+aHR0cDovL2NlcnRp
```

```
ZmljYXRlcy5nb2RhZGR5LmNvbS9yZXBvc2l0b3J5L2dkX2ludGVybWVkaWF0ZS5j
cnQwHwYDVR0jBBgwFoAU/axhMpNsRdbi7oVfmrrndplozOcwMwYDVR0RBCwwKoIR
bWFpbC5uaXhjcmFmdC5uZXSCFXd3dy5tYWlsLm5peGNyYWZ0Lm5ldDAdBgNVHQ4E
FgQUAYML0uoVH8Sn8JZ3xbR9NLzE0tYwDQYJKoZIhvcNAQEFBQADggEBAJ/1/mGM
tF/UPwOvmiNE0i46qXCJDs6Ui7kCxWWQzC+CbT6x3fe8VwZ2/9OVeScw5aGkG7sU
kfid0XmfXxYrqkVsubrhQt/1MKKowB35M5a/wRd7E0h2ucYhBF3dnTQ29yJ9ppHC
HOvsUDGOan+e7japMyTYn9PU9Y8QtnzovRXk55iYfL4p57YvPwk4yMnBtc/krQcd
m6ZdvmY+zbbjWaDyarfIp3fQCL2HD/lC5rJaGUn633GIT0OrrQ4Gfy6hQ98UC+Pt
I8LFuzs02dJlCpDhGquvQ0W6o4uuvjSP28HfGBcmKholG0GT9wyZZCBvUlFyV6kq
/KNTisOW4so6I+Q=
-----END CERTIFICATE-----
---
Server certificate
subject=/O=mail.nixcraft.net/CN=mail.nixcraft.net/OU=Domain Control Validated
issuer=/C=US/ST=Arizona/L=Scottsdale/O=GoDaddy.com, Inc./OU=http://certificates.godaddy.com
---
No client certificate CA names sent
---
SSL handshake has read 1823 bytes and written 316 bytes
---
New, TLSv1/SSLv3, Cipher is DHE-RSA-AES256-SHA
Server public key is 1024 bit
Compression: NONE
Expansion: NONE
SSL-Session:
    Protocol  : TLSv1
    Cipher    : DHE-RSA-AES256-SHA
    Session-ID: BF3662B2C597A7473E477D0CAD2D5002FCC370661BA5A7364BDCDD9C1247C0F5
    Session-ID-ctx:
    Master-Key: BFF4A2556DB4D7810D63DFF1905A97215185E94A791A2385A20290067F60208F108E54B0BC1
    Key-Arg   : None
    Start Time: 1243050920
    Timeout   : 300 (sec)
    Verify return code: 21 (unable to verify the first certificate)
```

Copy from the "-----BEGIN CERTIFICATE-----" to the "-----END CERTIFICATE-----" , and save it in your ~/.cert/mail.nixcraft.net/ directory as mail.nixcraft.net.pem.

Step # 2: Getting The Certificate Of The Issuer

This certificate was issued by Go Daddy, so you need to get "Certification Authority Root Certificate" (visit your CA's website to get root certificate):

```
$ wget https://certs.godaddy.com/repository/gd_bundle.crt -O
~/.cert/mail.nixcraft.net/gd.pem
```

Step # 3: Rehashing The Certificates

Create symbolic links to files named by the hash values using c_rehash, enter:

```
$ c_rehash ~/.cert/mail.nixcraft.net/
```

Sample output:

```
Doing  ~/.cert/mail.nixcraft.net/
mail.nixcraft.net.pem => 1d97af50.0
gd.pem => 219d9499.0
```

Test It

To confirm you have the correct and working certificates, enter:

```
$ openssl s_client -CApath ~/.cert/mail.nixcraft.net/ -connect mail.nixcraft.net:443
```

Sample output:

```
CONNECTED(00000003)
depth=3 /L=ValiCert Validation Network/O=ValiCert, Inc./OU=ValiCert Class 2 Policy Validati
verify return:1
depth=2 /C=US/O=The Go Daddy Group, Inc./OU=Go Daddy Class 2 Certification Authority
verify return:1
depth=1 /C=US/ST=Arizona/L=Scottsdale/O=GoDaddy.com, Inc./OU=http://certificates.godaddy.co
verify return:1
depth=0 /O=mail.nixcraft.net/CN=mail.nixcraft.net/OU=Domain Control Validated
verify return:1
---
Certificate chain
 0 s:/O=mail.nixcraft.net/CN=mail.nixcraft.net/OU=Domain Control Validated
   i:/C=US/ST=Arizona/L=Scottsdale/O=GoDaddy.com, Inc./OU=http://certificates.godaddy.com/r
---
Server certificate
-----BEGIN CERTIFICATE-----
MIIE5zCCA8+gAwIBAgIEAOJk2zANBgkqhkiG9w0BAQUFADCByjELMAkGA1UEBhMC
VVMxEDAOBgNVBAgTB0FyaXpvbmExEzARBgNVBAcTClNjb3R0c2RhbGUxGjAYBgNV
BAoTEUdvRGFkZHkuY29tLCBJbmMuMTMwMQYDVQQLEypodHRwOi8vY2VydGlmaWNh
dGVzLmdvZGFkZHkuY29tL3JlcG9zaXRvcnkxMDAuBgNVBAMTJ0dvIERhZGR5IFNl
Y3VyZSBDZXJ0aWZpY2F0aW9uIEF1dGhvcml0eTERMA8GA1UEBRMIMDc5NjkyODcw
HhcNMDkwMTE4MjEyMjMxWhcNMTEwMTE4MjEyMjMxWjBbMRowGAYDVQQKExFtYWls
Lm5peGNyYWZ0Lm5ldDEaMBgGA1UEAxMRbWFpbC5uaXhjcmFmdC5uZXQxITAfBgNV
BAsTGERvbWFpbiBDb250cm9sIFZhbGlkYXRlZDCBnzANBgkqhkiG9w0BAQEFAAOB
jQAwgYkCgYEA0LhCDXvNXhTHov9Szh474Cv3Nz7QspVOI4p5M+zZt18VTVCHJz0Z
TleJum8RblpU4NPHJgOauIb1CAE3vLSKySV2DjHMt2L2/NUatJiKjDQKAEloKwQK
t75BP0mAGFPZmHlMNUQ32Sr/0byxxM4ElL2SSBasJE3PPVkSBOtLfssCAwEAAaOC
AcUwggHBMA8GA1UdEwEB/wQFMAMBAQAwHQYDVR0lBBYwFAYIKwYBBQUHAwEGCCsG
AQUFBwMCMA4GA1UdDwEB/wQEAwIFoDAyBgNVHR8EKzApMCegJaAjhiFodHRwOi8v
Y3JsLmdvZGFkZHkuY29tL2dkczEtMS5jcmwwUwYDVR0gBEwwSjBIBgtghkgBhv1t
AQcXATA5MDcGCCsGAQUFBwIBFitodHRwOi8vY2VydGlmaWNhdGVzLmdvZGFkZHku
Y29tL3JlcG9zaXRvcnkvMIGABggrBgEFBQcBAQR0MHIwJAYIKwYBBQUHMAGGGGh0
dHA6Ly9vY3NwLmdvZGFkZHkuY29tLzBKBggrBgEFBQcwAoY+aHR0cDovL2NlcnRp
ZmljYXRlcy5nb2RhZGR5LmNvbS9yZXBvc2l0b3J5L2dkX2ludGVybWVkaWF0ZS5j
cnQwHwYDVR0jBBgwFoAU/axhMpNsRdbi7oVfmrrndplozOcwMwYDVR0RBCwwKoIR
bWFpbC5uaXhjcmFmdC5uZXSCFXd3dy5tYWlsLm5peGNyYWZ0Lm5ldDAdBgNVHQ4E
FgQUAYML0uoVH8Sn8JZ3xbR9NLzE0tYwDQYJKoZIhvcNAQEFBQADggEBAJ/1/mGM
tF/UPwOvmiNE0i46qXCJDs6Ui7kCxWWQzC+CbT6x3fe8VwZ2/9OVeScw5aGkG7sU
kfid0XmfXxYrqkVsubrhQt/1MKKowB35M5a/wRd7E0h2ucYhBF3dnTQ29yJ9ppHC
HOvsUDGOan+e7japMyTYn9PU9Y8QtnzovRXk55iYfL4p57YvPwk4yMnBtc/krQcd
m6ZdvmY+zbbjWaDyarfIp3fQCL2HD/lC5rJaGUn633GIT0OrrQ4Gfy6hQ98UC+Pt
I8LFuzs02dJlCpDhGquvQ0W6o4uuvjSP28HfGBcmKholG0GT9wyZZCBvUlFyV6kq
/KNTisOW4so6I+Q=
-----END CERTIFICATE-----
subject=/O=mail.nixcraft.net/CN=mail.nixcraft.net/OU=Domain Control Validated
issuer=/C=US/ST=Arizona/L=Scottsdale/O=GoDaddy.com, Inc./OU=http://certificates.godaddy.com
---
No client certificate CA names sent
---
SSL handshake has read 1823 bytes and written 316 bytes
---
New, TLSv1/SSLv3, Cipher is DHE-RSA-AES256-SHA
Server public key is 1024 bit
Compression: NONE
Expansion: NONE
SSL-Session:
    Protocol  : TLSv1
    Cipher    : DHE-RSA-AES256-SHA
    Session-ID: 37E5AF0EE1745AB2DACAEE0FB7824C178A58C6AEF7A0EF93609643F16A20EE51
    Session-ID-ctx:
    Master-Key: 7B9F8A79D3CC3A41CA572ED266076A1531E12EE8D07D859D65F24368ABA0D2CAE670AA06524
    Key-Arg   : None
    Start Time: 1243051912
    Timeout   : 300 (sec)
    Verify return code: 0 (ok)
---
```

There should be lots of data, however the important thing to note down is that the final line "Verify return code: 0 (ok)".

I'm using the same certificate for dovecot IMAP mail server, type the following to verify mail server SSL certificate:

```
$ openssl s_client -CApath ~/.cert/mail.nixcraft.net/ -connect mail.nixcraft.net:993
```

Sample output:

```
CONNECTED(00000003)
depth=2 /C=US/O=The Go Daddy Group, Inc./OU=Go Daddy Class 2 Certification Authority
verify return:1
depth=1 /C=US/ST=Arizona/L=Scottsdale/O=GoDaddy.com, Inc./OU=http://certificates.godaddy.co
verify return:1
depth=0 /O=mail.nixcraft.net/CN=mail.nixcraft.net/OU=Domain Control Validated
verify return:1
---
Certificate chain
 0 s:/O=mail.nixcraft.net/CN=mail.nixcraft.net/OU=Domain Control Validated
   i:/C=US/ST=Arizona/L=Scottsdale/O=GoDaddy.com, Inc./OU=http://certificates.godaddy.com/r
 1 s:/C=US/ST=Arizona/L=Scottsdale/O=GoDaddy.com, Inc./OU=http://certificates.godaddy.com/r
   i:/C=US/O=The Go Daddy Group, Inc./OU=Go Daddy Class 2 Certification Authority
---
Server certificate
-----BEGIN CERTIFICATE-----
MIIE5zCCA8+gAwIBAgIEAOJk2zANBgkqhkiG9w0BAQUFADCByjELMAkGA1UEBhMC
VVMxEDAOBgNVBAgTB0FyaXpvbmExEzARBgNVBAcTClNjb3R0c2RhbGUxGjAYBgNV
BAoTEUdvRGFkZHkuY29tLCBJbmMuMTMwMQYDVQQLEypodHRwOi8vY2VydGlmaWNh
dGVzLmdvZGFkZHkuY29tL3JlcG9zaXRvcnkxMDAuBgNVBAMTJ0dvIERhZGR5IFNl
Y3VyZSBDZXJ0aWZpY2F0aW9uIEF1dGhvcml0eTERMA8GA1UEBRMIMDc5NjkyODcw
HhcNMDkwMTE4MjEyMjMxWhcNMTEwMTE4MjEyMjMxWjBbMRowGAYDVQQKExFtYWls
Lm5peGNyYWZ0Lm5ldDEaMBgGA1UEAxMRbWFpbC5uaXhjcmFmdC5uZXQxITAfBgNV
BAsTGERvbWFpbiBDb250cm9sIFZhbGlkYXRlZDCBnzANBgkqhkiG9w0BAQEFAAOB
jQAwgYkCgYEA0LhCDXvNXhTHov9Szh474Cv3Nz7QspVOI4p5M+zZt18VTVCHJz0Z
TleJum8RblpU4NPHJgOauIb1CAE3vLSKySV2DjHMt2L2/NUatJiKjDQKAEloKwQK
t75BP0mAGFPZmHlMNUQ32Sr/0byxxM4ElL2SSBasJE3PPVkSBOtLfssCAwEAAaOC
AcUwggHBMA8GA1UdEwEB/wQFMAMBAQAwHQYDVR0lBBYwFAYIKwYBBQUHAwEGCCsG
AQUFBwMCMA4GA1UdDwEB/wQEAwIFoDAyBgNVHR8EKzApMCegJaAjhiFodHRwOi8v
Y3JsLmdvZGFkZHkuY29tL2dkczEtMS5jcmwwUwYDVR0gBEwwSjBIBgtghkgBhv1t
AQcXATA5MDcGCCsGAQUFBwIBFitodHRwOi8vY2VydGlmaWNhdGVzLmdvZGFkZHku
Y29tL3JlcG9zaXRvcnkvMIGABggrBgEFBQcBAQR0MHIwJAYIKwYBBQUHMAGGGGh0
dHA6Ly9vY3NwLmdvZGFkZHkuY29tLzBKBggrBgEFBQcwAoY+aHR0cDovL2NlcnRp
ZmljYXRlcy5nb2RhZGR5LmNvbS9yZXBvc2l0b3J5L2dkX2ludGVybWVkaWF0ZS5j
cnQwHwYDVR0jBBgwFoAU/axhMpNsRdbi7oVfmrrndplozOcwMwYDVR0RBCwwKoIR
bWFpbC5uaXhjcmFmdC5uZXSCFXd3dy5tYWlsLm5peGNyYWZ0Lm5ldDADBgNVHQ4E
FgQUAYML0uoVH8Sn8JZ3xbR9NLzE0tYwDQYJKoZIhvcNAQEFBQADggEBAJ/1/mGM
tF/UPwOvmiNE0i46qXCJDs6Ui7kCxWWQzC+CbT6x3fe8VwZ2/9OVeScw5aGkG7sU
kfid0XmfXxYrqkVsubrhQt/1MKKowB35M5a/wRd7E0h2ucYhBF3dnTQ29yJ9ppHC
HOvsUDGOan+e7japMyTYn9PU9Y8QtnzovRXk55iYfL4p57YvPwk4yMnBtc/krQcd
m6ZdvmY+zbbjWaDyarfIp3fQCL2HD/lC5rJaGUn633GIT0OrrQ4Gfy6hQ98UC+Pt
I8LFuzs02dJlCpDhGquvQ0W6o4uuvjSP28HfGBcmKholG0GT9wyZZCBvUlFyV6kq
/KNTisOW4so6I+Q=
-----END CERTIFICATE-----
subject=/O=mail.nixcraft.net/CN=mail.nixcraft.net/OU=Domain Control Validated
issuer=/C=US/ST=Arizona/L=Scottsdale/O=GoDaddy.com, Inc./OU=http://certificates.godaddy.com
---
No client certificate CA names sent
---
SSL handshake has read 3076 bytes and written 316 bytes
---
New, TLSv1/SSLv3, Cipher is DHE-RSA-AES256-SHA
Server public key is 1024 bit
Compression: NONE
Expansion: NONE
SSL-Session:
    Protocol  : TLSv1
    Cipher    : DHE-RSA-AES256-SHA
    Session-ID: 509D310C0184E0540FC24F60F36D3E2A62C1F98D6367DBC62E8432FFDC79757A
    Session-ID-ctx:
    Master-Key: 72013A336DAFAF16917C4082785D3D9ADA3D0D3420B63FC5A6C9E5F44117D340A105165384
    Key-Arg   : None
    Start Time: 1243052074
```

```
    Timeout   : 300 (sec)
    Verify return code: 0 (ok)
---
* OK [CAPABILITY IMAP4rev1 SASL-IR SORT THREAD=REFERENCES MULTIAPPEND UNSELECT LITERAL+ IDI
```

Again the final "Dovecot ready" line along with 0 return code indicates that everything is working fine.