Installing a LetsEncrypt SSL Certificate

1. Zimbra Tech Center
2. Community Sandbox
3. Installing a LetsEncrypt SSL Certificate

Contents

- 1 Installing a Let's Encrypt SSL Certificate
  - 1.1 Purpose
  - 1.2 Resolution
    - 1.2.1 Installing Let's Encrypt on a Zimbra Server
    - 1.2.2 Where are the SSL Certificate Files?
    - 1.2.3 Build the proper Intermediate CA plus Root CA
    - 1.2.4 Verify your commercial certificate.
      - 1.2.4.1 Zimbra Collaboration 8.7 and above
      - 1.2.4.2 Zimbra Collaboration 8.6 and previous
    - 1.2.5 Deploy the new Let's Encrypt SSL certificate
      - 1.2.5.1 Backup Zimbra SSL directory
      - 1.2.5.2 Copy the private key under Zimbra SSL path
      - 1.2.5.3 Final SSL deployment
        - 1.2.5.3.1 Zimbra Collaboration 8.7 and above
        - 1.2.5.3.2 Zimbra Collaboration 8.6 and previous
    - 1.2.6 Test the new SSL Certificate
    - 1.2.7 Test the new SSL Certificate with OpenSSL
    - 1.2.8 Building Multi-SAN SSL Certificate and complex scenarios
    - 1.2.9 Verifying SSL certificate is not expired
  - 1.3 Additional Content
- 2 Automatic methods

Installing a Let's Encrypt SSL Certificate

zimbra
A SYNACOR PRODUCT
Let's Encrypt
Zimbra: Installing a
Let's Encrypt SSL Certificate
Let's Encrypt is now Public Beta, and it works
perfect on Zimbra Servers. You can try it now
following the next steps. *For Staging and Test

Purpose

Step by Step Wiki/KB article to install a Let's Encrypt Commercial Certificate. **Disclaimer** The Let's Encrypt Client is **BETA SOFTWARE**. It contains plenty of bugs and rough edges, and it should be tested thoroughly in staging environments before use on production systems. For more information regarding the status of the project, please see https://letsencrypt.org. Be sure to check out the Frequently Asked Questions (FAQ) (https://community.letsencrypt.org/t/frequently-asked-questions-faq/26#topic-title).

Resolution

Let's Encrypt is a new Certificate Authority: It's free, automated, and open. It could be an option to protect Zimbra Servers with a valid SSL certificate; however, please be aware that is a Beta for now. Some stuff could not work or have issues, so use it at your own risk.

Installing Let's Encrypt on a Zimbra Server

Let's Encrypt must be installed on one Linux machine to obtain the proper SSL Certificate, CA Intermediate, and Private Key. It is not required that it be on the same Zimbra Server, but it could save time and help to obtain the renewals, etc.

- First Step is to stop the jetty or nginx service at Zimbra level

```
zmproxyctl stop
zmmailboxdctl stop
```

- Second step is to Install git on the Server (apt-get install git/yum install git), and then do a git clone of the project on the folder we want
  - Note: On RedHat/CentOS 6 you will need to enable the EPEL repository before install.

```
git clone https://github.com/letsencrypt/letsencrypt
cd letsencrypt
```

- Let's now run Let's Encrypt in auto mode and use the certonly option, because for now the project can't automatically install the cert on Zimbra servers.

```
root@zimbra86:~/tmp/letsencrypt# ./letsencrypt-auto certonly --standalone
```

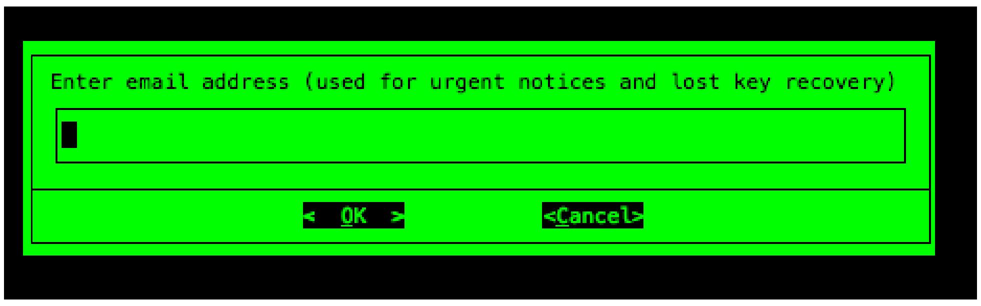
If you need to have multiple hostnames on the same SSL, so a Multi-SAN, SSL, please run instead, where -d are your domains:

```
root@zimbra86:~/tmp/letsencrypt# ./letsencrypt-auto certonly --standalone -d xmpp.example.com -d conference.example.com
```

- - (This step only happens the first time. This process will not occur when renewing the SSL Certificate if using the same machine.) The process will download all of the OS dependencies that Let's Encrypt needs, and after a few minutes:

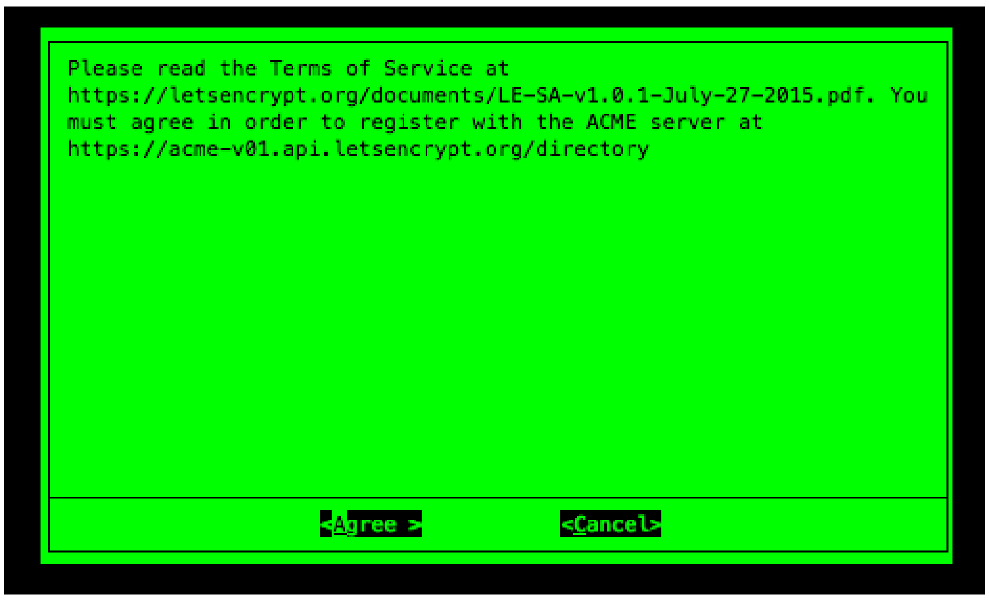
```
Creating virtual environment...
Updating letsencrypt and virtual environment dependencies...../root/.local/share/letsencrypt/local/lib/python2.7/site-packages/pip/_vendor/requests/packages/ur
  InsecurePlatformWarning
./root/.local/share/letsencrypt/local/lib/python2.7/site-packages/pip/_vendor/requests/packages/urllib3/util/ssl_.py:90: InsecurePlatformWarning: A true SSLCon
  InsecurePlatformWarning
```

- - - The process will ask for an Email Address in case of emergency contact or to recover the lost key.



Enter email address (used for urgent notices and lost key recovery)

- - - The process will ask if we agree with the ToS.

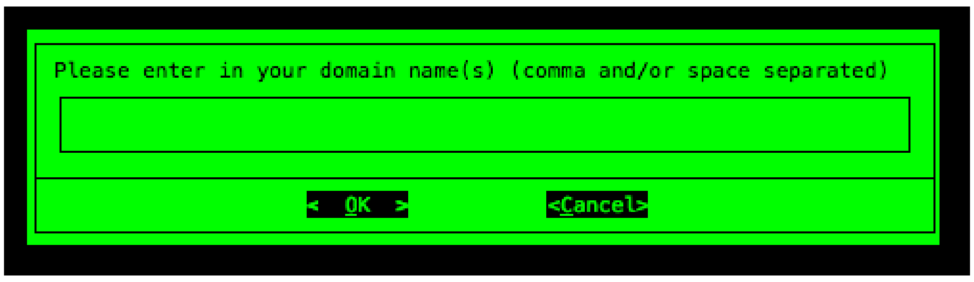


Please read the Terms of Service at https://letsencrypt.org/documents/LE-SA-v1.0.1-July-27-2015.pdf. You must agree in order to register with the ACME server at https://acme-v01.api.letsencrypt.org/directory

- - - - In case we run a renewal, or a request for a new FQDN, the process will just take a few seconds.

```
Updating letsencrypt and virtual environment dependencies.......
Running with virtualenv: /root/.local/share/letsencrypt/bin/letsencrypt certonly
```

- - - Let's Encrypt will prompt for the domain to protect, in this lab case (zimbra86.zimbra.io):



Please enter in your domain name(s) (comma and/or space separated)

- The process will take a few seconds to validate and then will end:

```
IMPORTANT NOTES:
 - Congratulations! Your certificate and chain have been saved at
   /etc/letsencrypt/live/zimbra86.zimbra.io/fullchain.pem. Your cert
   will expire on 2016-03-04. To obtain a new version of the
   certificate in the future, simply run Let's Encrypt again.
 - If like Let's Encrypt, please consider supporting our work by:

   Donating to ISRG / Let's Encrypt:   https://letsencrypt.org/donate
   Donating to EFF:                    https://eff.org/donate-le
```

Where are the SSL Certificate Files?

You can find all your files under **/etc/letsencrypt/live/$domain**, where $domain is the fqdn you used during the process:

```
root@zimbra86:/etc/letsencrypt/live/zimbra86.zimbra.io# ls -al
total 8
drwxr-xr-x 2 root root 4096 Dec  5 16:46 .
drwx------ 3 root root 4096 Dec  5 16:46 ..
lrwxrwxrwx 1 root root   42 Dec  5 16:46 cert.pem -> ../../archive/zimbra86.zimbra.io/cert1.pem
lrwxrwxrwx 1 root root   43 Dec  5 16:46 chain.pem -> ../../archive/zimbra86.zimbra.io/chain1.pem
lrwxrwxrwx 1 root root   47 Dec  5 16:46 fullchain.pem -> ../../archive/zimbra86.zimbra.io/fullchain1.pem
lrwxrwxrwx 1 root root   45 Dec  5 16:46 privkey.pem -> ../../archive/zimbra86.zimbra.io/privkey1.pem
```

cert.pem is the certificate

chain.pem is the chain

fullchain.pem is the concatenation of cert.pem + chain.pem

privkey.pem is the private key

Please keep in mind that the private key is only for you.

Build the proper Intermediate CA plus Root CA

Let's Encrypt is almost perfect, but during the files the process built, they just add the chain.pem file without the root CA. You must to use the IdenTrust root Certificate and merge it after the chain.pem

- https://www.identrust.com/certificates/trustid/root-download-x3.html

Your chain.pem should look like:

```
-----BEGIN CERTIFICATE-----
YOURCHAIN
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIDSjCCAjKgAwIBAgIQRK+wgNajJ7qJMDmGLvhAazANBgkqhkiG9w0BAQUFADA/
MSQwIgYDVQQKExtEaWdpdGFsIFNpZ25hdHVyZSBUcnVzdCBDby4xFzAVBgNVBAMT
DkRTVCBSb290IENBIFgzMB4XDTAwMDkzMDIxMTIxOVoXDTIxMDkzMDE0MDExNVow
PzEkMCIGA1UEChMbRGlnaXRhbCBTaWduYXR1cmUgVHJ1c3QgQ28uMRcwFQYDVQQD
Ew5EU1QgUm9vdCBDQSBYMzCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB
AN+v6ZdQCINXtMxiZfaQguzH0yxrMMpb7NnDfcdAwRgUi+DoM3ZJKuM/IUmTrE4O
rz5Iy2Xu/NMhD2XSKtkyj4zl93ewEnu1lcCJo6m67XMuegwGMoOifooUMM0RoOEq
OLl5CjH9UL2AZd+3UWODyOKIYepLYYHsUmu5ouJLGiifSKOeDNoJjj4XLh7dIN9b
xiqKqy69cK3FCxolkHRyxXtqqzTWMIn/5WgTe1QLyNau7Fqckh49ZLOMxt+/yUFw
7BZy1SbsOFU5Q9D8/RhcQPGX69Wam40dutolucbY38EVAjqr2m7xPi71XAicPNaD
aeQQmxkqtilX4+U9m5/wAl0CAwEAAaNCMEAwDwYDVR0TAQH/BAUwAwEB/zAOBgNV
HQ8BAf8EBAMCAQYwHQYDVR0OBBYEFMSnsaR7LHH62+FLkHX/xBVghYkQMA0GCSqG
SIb3DQEBBQUAA4IBAQCjGiybFwBcqR7uKGY3Or+Dxz9LwwmglSBd49lZRNI+DT69
ikugdB/OEIKcdBodfpga3csTS7MgROSR6cz8faXbauX+5v3gTt23ADq1cEmv8uXr
AvHRAosZy5Q6XkjEGB5YGV8eAlrwDPGxrancWYaLbumR9YbK+rlmM6pZW87ipxZz
R8srzJmwN0jP41ZL9c8PDHIyh8bwRLtTcm1D9SZImlJnt1ir/md2cXjbDaJWFBM5
JDGFoqgCWjBH4d1QB7wCCZAA62RjYJsWvIjJEubSfZGL+T0yjWW06XyxV3bqxbYo
Ob8VZRzI9neWagqNdwvYkQsEjgfbKbYK7p2CNTUQ
-----END CERTIFICATE-----
```

To sum up: chain.pem has to be concatened with the root CA. First the chain and the end of the file the root CA. The order is important.

Verify your commercial certificate.

Copy all the Let's Encrypt folder with all files **/etc/letsencrypt/live/$domain** into /opt/zimbra/ssl/letsencrypt:

```
root@mail2:~# mkdir /opt/zimbra/ssl/letsencrypt
root@mail2:~# cp /etc/letsencrypt/live/mail2.next.zimbra.io/* /opt/zimbra/ssl/letsencrypt/
root@mail2:~# chown zimbra:zimbra /opt/zimbra/ssl/letsencrypt/*
root@mail2:~# ls -la /opt/zimbra/ssl/letsencrypt/
total 24
drwxr-xr-x 2 root   root   4096 Jul 15 22:59 .
drwxr-xr-x 8 zimbra zimbra 4096 Jul 15 22:59 ..
-rw-r--r-- 1 zimbra zimbra 1809 Jul 15 22:59 cert.pem
-rw-r--r-- 1 zimbra zimbra 2847 Jul 15 22:59 chain.pem
-rw-r--r-- 1 zimbra zimbra 3456 Jul 15 22:59 fullchain.pem
-rw-r--r-- 1 zimbra zimbra 1704 Jul 15 22:59 privkey.pem
```

Zimbra Collaboration 8.7 and above

As **zimbra** user

```
zimbra@zimbra87:/opt/zimbra/ssl/letsencrypt/# /opt/zimbra/bin/zmcertmgr verifycrt comm privkey.pem cert.pem chain.pem
** Verifying cert.pem against privkey.pem
Certificate (cert.pem) and private key (privkey.pem) match.
Valid Certificate: cert.pem: OK
```

Zimbra Collaboration 8.6 and previous

As **root** user

```
root@zimbra86:/opt/zimbra/ssl/letsencrypt/# /opt/zimbra/bin/zmcertmgr verifycrt comm privkey.pem cert.pem chain.pem
** Verifying cert.pem against privkey.pem
Certificate (cert.pem) and private key (privkey.pem) match.
Valid Certificate: cert.pem: OK
```

Deploy the new Let's Encrypt SSL certificate

Backup Zimbra SSL directory

Before deploying a good practice is to make a backup.

```
cp -a /opt/zimbra/ssl/zimbra /opt/zimbra/ssl/zimbra.$(date "+%Y%m%d")
```

Copy the private key under Zimbra SSL path

Before deploying the SSL Certificate, you need to move the privkey.pem under the Zimbra SSL commercial path, like this:

```
cp /opt/zimbra/ssl/letsencrypt/privkey.pem /opt/zimbra/ssl/zimbra/commercial/commercial.key
```

Final SSL deployment

Then deploy the certificate as follows:

Zimbra Collaboration 8.7 and above

As **zimbra** user

```
zimbra@mail2://opt/zimbra/ssl/letsencrypt/$ /opt/zimbra/bin/zmcertmgr deploycrt comm cert.pem chain.pem
** Verifying 'cert.pem' against '/opt/zimbra/ssl/zimbra/commercial/commercial.key'
Certificate 'cert.pem' and private key '/opt/zimbra/ssl/zimbra/commercial/commercial.key' match.
** Verifying 'cert.pem' against 'chain.pem'
Valid certificate chain: cert.pem: OK
** Copying 'cert.pem' to '/opt/zimbra/ssl/zimbra/commercial/commercial.crt'
** Copying 'chain.pem' to '/opt/zimbra/ssl/zimbra/commercial/commercial_ca.crt'
** Appending ca chain 'chain.pem' to '/opt/zimbra/ssl/zimbra/commercial/commercial.crt'
** Importing cert '/opt/zimbra/ssl/zimbra/commercial/commercial_ca.crt' as 'zcs-user-commercial_ca' into cacerts '/opt/zimbra/common/lib/jvm/java/jre/lib/secur
** NOTE: restart mailboxd to use the imported certificate.
** Saving config key 'zimbraSSLCertificate' via zmprov modifyServer mail2.next.zimbra.io...failed (rc=1)
** Installing ldap certificate '/opt/zimbra/conf/slapd.crt' and key '/opt/zimbra/conf/slapd.key'
** Copying '/opt/zimbra/ssl/zimbra/commercial/commercial.crt' to '/opt/zimbra/conf/slapd.crt'
** Copying '/opt/zimbra/ssl/zimbra/commercial/commercial.key' to '/opt/zimbra/conf/slapd.key'
** Creating file '/opt/zimbra/ssl/zimbra/jetty.pkcs12'
** Creating keystore '/opt/zimbra/mailboxd/etc/keystore'
** Installing mta certificate '/opt/zimbra/conf/smtpd.crt' and key '/opt/zimbra/conf/smtpd.key'
** Copying '/opt/zimbra/ssl/zimbra/commercial/commercial.crt' to '/opt/zimbra/conf/smtpd.crt'
** Copying '/opt/zimbra/ssl/zimbra/commercial/commercial.key' to '/opt/zimbra/conf/smtpd.key'
** Installing proxy certificate '/opt/zimbra/conf/nginx.crt' and key '/opt/zimbra/conf/nginx.key'
** Copying '/opt/zimbra/ssl/zimbra/commercial/commercial.crt' to '/opt/zimbra/conf/nginx.crt'
** Copying '/opt/zimbra/ssl/zimbra/commercial/commercial.key' to '/opt/zimbra/conf/nginx.key'
** NOTE: restart services to use the new certificates.
** Cleaning up 3 files from '/opt/zimbra/conf/ca'
** Removing /opt/zimbra/conf/ca/41b01cbb.0
** Removing /opt/zimbra/conf/ca/ca.key
** Removing /opt/zimbra/conf/ca/ca.pem
** Copying CA to /opt/zimbra/conf/ca
** Copying '/opt/zimbra/ssl/zimbra/ca/ca.key' to '/opt/zimbra/conf/ca/ca.key'
** Copying '/opt/zimbra/ssl/zimbra/ca/ca.pem' to '/opt/zimbra/conf/ca/ca.pem'
** Creating CA hash symlink '41b01cbb.0' -> 'ca.pem'
** Creating /opt/zimbra/conf/ca/commercial_ca_1.crt
** Creating CA hash symlink '4f06f81d.0' -> 'commercial_ca_1.crt'
** Creating /opt/zimbra/conf/ca/commercial_ca_2.crt
** Creating CA hash symlink '2e5ac55d.0' -> 'commercial_ca_2.crt'
```

Zimbra Collaboration 8.6 and previous

As **root** user

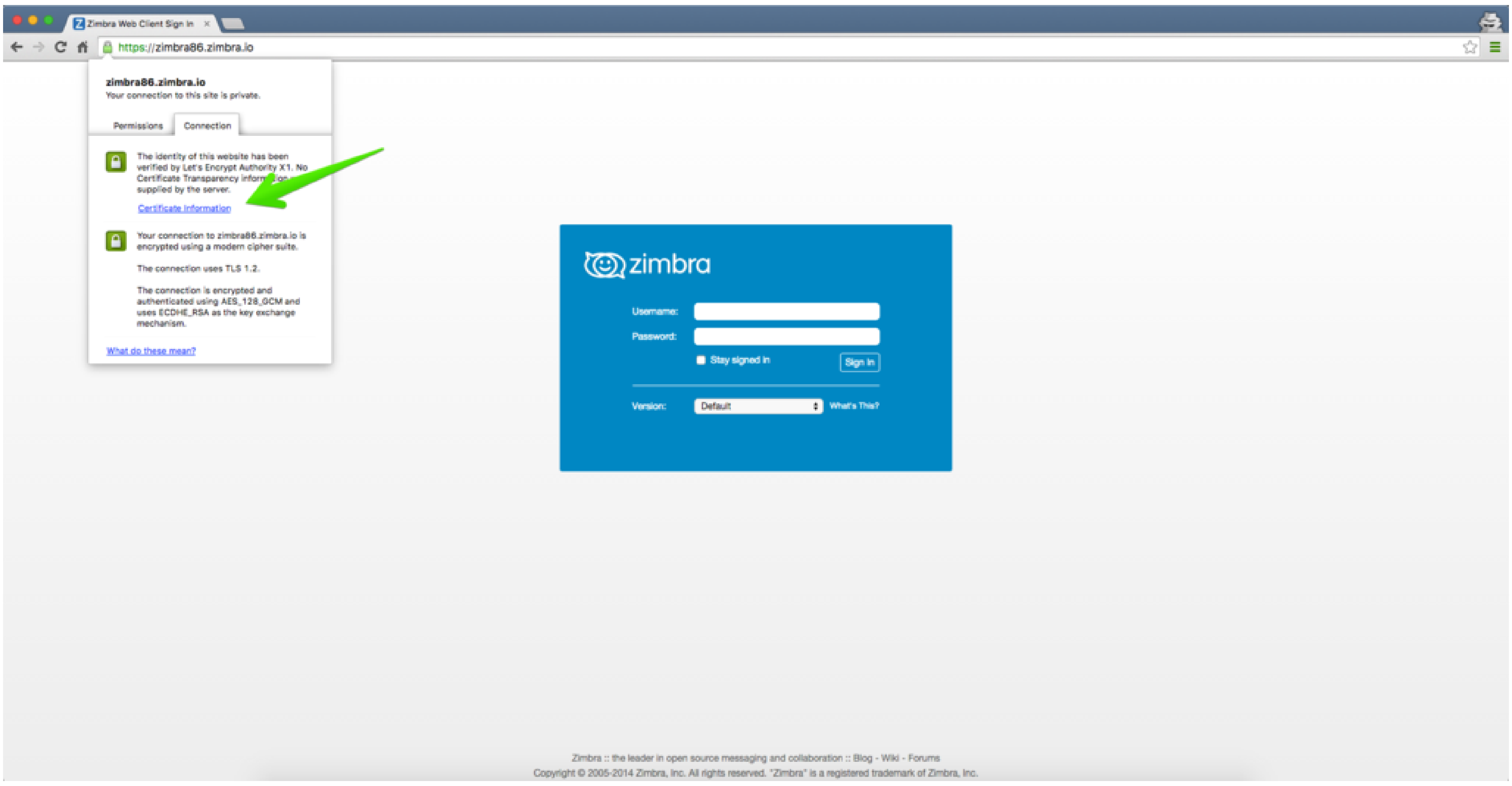
```
root@zimbra86:/opt/zimbra/ssl/letsencrypt/# /opt/zimbra/bin/zmcertmgr deploycrt comm cert.pem chain.pem
** Verifying cert.pem against /opt/zimbra/ssl/zimbra/commercial/commercial.key
Certificate (cert.pem) and private key (/opt/zimbra/ssl/zimbra/commercial/commercial.key) match.
Valid Certificate: cert.pem: OK
** Copying cert.pem to /opt/zimbra/ssl/zimbra/commercial/commercial.crt
** Appending ca chain chain.pem to /opt/zimbra/ssl/zimbra/commercial/commercial.crt
** Importing certificate /opt/zimbra/ssl/zimbra/commercial/commercial_ca.crt to CACERTS as zcs-user-commercial_ca...done.
** NOTE: mailboxd must be restarted in order to use the imported certificate.
** Saving server config key zimbraSSLCertificate...failed.
** Saving server config key zimbraSSLPrivateKey...failed.
** Installing mta certificate and key...done.
** Installing slapd certificate and key...done.
** Installing proxy certificate and key...done.
** Creating pkcs12 file /opt/zimbra/ssl/zimbra/jetty.pkcs12...done.
** Creating keystore file /opt/zimbra/mailboxd/etc/keystore...done.
** Installing CA to /opt/zimbra/conf/ca...done.
```

Then you need to restart the services, which will restart the nginx or jetty you stopped before:

```
zmcontrol restart
```

Test the new SSL Certificate

The last step is to go to your Web Browser and open the URL of your Zimbra server where you installed the Let's Encrypt SSL Certificate:



zimbra86.zimbra.io
Your connection to this site is private.

The identity of this website has been verified by Let's Encrypt Authority X1. No Certificate Transparency inform[illegible]on [illegible] supplied by the server.

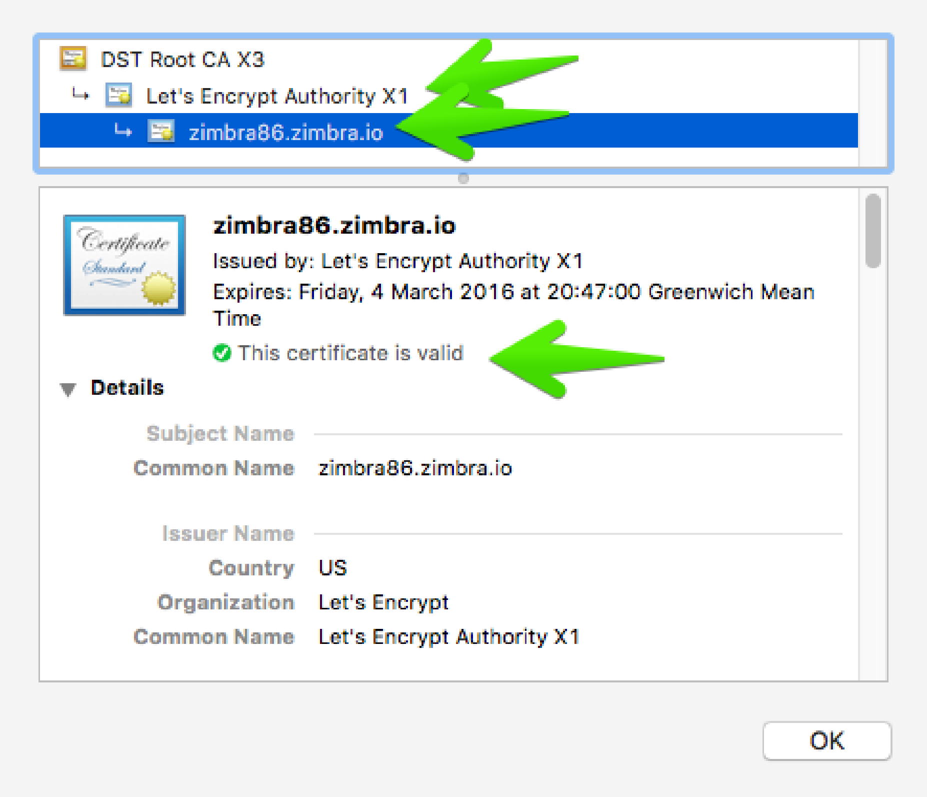
Your connection to zimbra86.zimbra.io is encrypted using a modern cipher suite.

The connection uses TLS 1.2.

The connection is encrypted and authenticated using AES_128_GCM and uses ECDHE_RSA as the key exchange mechanism.

Zimbra :: the leader in open source messaging and collaboration :: Blog - Wiki - Forums
Copyright © 2005-2014 Zimbra, Inc. All rights reserved. "Zimbra" is a registered trademark of Zimbra, Inc.

You can expand the Certificate Information to see the new SSL Certificate your server is using:



DST Root CA X3
↳ Let's Encrypt Authority X1
↳ zimbra86.zimbra.io

zimbra86.zimbra.io
Issued by: Let's Encrypt Authority X1
Expires: Friday, 4 March 2016 at 20:47:00 Greenwich Mean Time
✓ This certificate is valid

▼ **Details**

Subject Name
Common Name zimbra86.zimbra.io

Issuer Name
Country US
Organization Let's Encrypt
Common Name Let's Encrypt Authority X1

Test the new SSL Certificate with OpenSSL

You can use openssl cli tools to check and test the new SSL certificate:

```
echo QUIT | openssl s_client -connect $domain:443 | openssl x509 -noout -text | less
```

where $domain is the fqdn you used during the process

Building Multi-SAN SSL Certificate and complex scenarios

You can do almost everything you need, like Subject Alt Names, different domains, etc. But to see more about this, visit the web of the official project (https://letsencrypt.org/).

Here is an example using two FQDN:

```
./letsencrypt-auto certonly --standalone -d fqdn1 -d fqdn2
```

Verifying SSL certificate is not expired

SSL certificates issued by let's encrypt are valid for 90 days during the BETA phase. You need to check the expiration of your SSL certificate. We can suggest using monitoring tools like Nagios. With nagios plugins there's a command which can check the expiration:

```
/usr/lib/nagios/plugins/check_http --sni -H '<FQDN>' -C 30,14
```

A warning will be issued 30 days before the expiration, a critical will be issued 14 days before the expiration.

Here is a nagios config file excerpt:

```
define command{
        command_name    check_https_vhost
        command_line    /usr/lib/nagios/plugins/check_http --sni -H '$ARG1$' -C 30,14
}
```

```
define service{
        use generic-service
        host_name <FQDN>
        service_description SSL <FQDN>
        check_command check_https_vhost!<FQDN>
}
```

Additional Content

- Let's Encrypt User Manual - https://letsencrypt.readthedocs.org/en/latest/using.html
- Let's Encrypt Official Project - https://letsencrypt.org/

Automatic methods

Since Letsencrypt has gone public several scripts were created to automate the deployment of free SSL certificates in Zimbra. In order of appearance:

- Vojtěch Myslivec on GitHub (https://github.com/VojtechMyslivec/letsencrypt-zimbra/)
- Grown from a long discussion on the forum (https://forums.zimbra.org/viewtopic.php?f=15&t=60781) Jim Dunphy developed a script (https://github.com/JimDunphy/deploy-zimbra-letsencrypt.sh) based on Neilpang's acme.sh script
- A nearly fully automated script developed by Maxxer@YetOpen on GitHub (https://github.com/yetopen/certbot-zimbra)

Retrieved from "https://wiki.zimbra.com/index.php?title=Installing_a_LetsEncrypt_SSL_Certificate&oldid=65017"

Categories: ZCS 8.8 | ZCS 8.7 | Community Sandbox | NeedSME | Certificates