Installing a Let's Encrypt SSL Certificate

KB 22434	Last updated on 2024-09-11	Last updated by Gautam	5.00 (one vote)	Verified in: ZCS 10.0 ZCS 9.0 ZCS 8.8

- This is **certified documentation** and is protected for editing by Zimbra Employees & Moderators only.

Contents

How to use Zimbra with Let's Encrypt certificates

This article is a step-by-step instruction on setting up a Zimbra with Let's Encrypt certificates.

If you are running a multi server installation of Zimbra it is recommended you set-up a dedicated VM for obtaining the Let's Encrypt certificate and follow the steps under `Manual installation of Let's Encrypt on Zimbra`.

Prerequisites

This guide assumes you are using Ubuntu 20 and you have set up a correct hostname and DNS, to check run the following as user `zimbra` and verify `zmhostname` is the same as `hostname --fqdn`:

```
zimbra@le-test:~$ source ~/bin/zmshutil; zmsetvars
zimbra@le-test:~$ zmhostname
le-test.zimbra.tech
zimbra@le-test:~$ hostname --fqdn
le-test.zimbra.tech
```

Next you should have set up a CAA DNS record so that Let's Encrypt can issue certificates for your domain, to check run the following and make sure `0 issue "letsencrypt.org"` is in the output of the command:

```
zimbra@le-test:~$ sudo apt install -y net-tools dnsutils
zimbra@le-test:~$ dig +short type257 ${hostname --d}
0 issuewild "letsencrypt.org"
0 issue "letsencrypt.org"
```

Next check if Zimbra listens on port 80, Let's Encrypt needs to be able to run a temporary webserver on port 80, so it can not be used by Zimbra. This is not an issue as most browsers now try https first. The following command should not have any output:

```
netstat -tulpn | grep ":80 "
```

In case your Zimbra is listening on port 80, you have to switch the proxy mode like this:

```
sudo su zimbra -
zmprov ms `zmhostname` zimbraReverseProxyMailMode https
zmprov ms `zmhostname` zimbraMailMode https
/opt/zimbra/bin/zmtlsctl https
/opt/zimbra/libexec/zmproxyconfig -e -w -o -a 8080:80:8443:443 -x https -H `zmhostname`
```

If you are having trouble setting up Zimbra you can use our automated installer that will take care of Let's Encrypt also: https://github.com/Zimbra/zinstaller

Further reading:

- https://wiki.zimbra.com/wiki/CLI_zmtlsctl_to_set_Web_Server_Mode
- https://wiki.zimbra.com/wiki/Enabling_Zimbra_Proxy_and_memcached

Installing Certbot

Certbot in the Ubuntu repositories is too old and cannot be used for Zimbra. The newer version can be installed via snap or pip. Run below commands to install Cerbot and obtain a certificate:

```
apt install -y python3 python3-venv libaugeas0
python3 -m venv /opt/certbot/
/opt/certbot/bin/pip install --upgrade pip
/opt/certbot/bin/pip install certbot
ln -s /opt/certbot/bin/certbot /usr/local/sbin/certbot
/usr/local/sbin/certbot certonly -d ${hostname --fqdn} --standalone --preferred-chain  "ISRG Root X2" --agree-tos --register-unsafely-without-email
```

Support for ECDSA TLS (elliptic curve cryptography ECC) certificates has been added to Zimbra `zmcertmgr` from Zimbra versions 10.0.6, Joule-8.8.15-Patch-45, Kepler-9.0.0-Patch-38. Let's Encrypt Certbot defaults to ECDSA secp256r1 (P-256) from version 2.0.0. If you are running out-of-date versions of the software or have another reason why you are required to use RSA certificates. Refer to https://wiki.zimbra.com/index.php?title=Installing_a_LetsEncrypt_SSL_Certificate&oldid=69351 at your own risk as we do not support/test or update documentation for out of date deployments.

Let's Encrypt also supports wildcard certificates. The DNS validation needs to be manual:

```
/usr/local/sbin/certbot certonly -d *.example.com --preferred-chain "ISRG Root X2" --agree-tos --register-unsafely-without-email --preferred-challenges=dns --manual
```

Zimbra deployment

Create the following script that deploys the Let's Encrypt certificate on Zimbra:

```
cat >> /usr/local/sbin/letsencrypt-zimbra << EOF
#!/bin/bash
/usr/local/sbin/certbot certonly -d ${hostname --fqdn} --standalone -n --preferred-chain  "ISRG Root X2" --agree-tos --register-unsafely-without-email
cp "/etc/letsencrypt/live/${hostname --fqdn}/privkey.pem" /opt/zimbra/ssl/zimbra/commercial/commercial.key
chown zimbra:zimbra /opt/zimbra/ssl/zimbra/commercial/commercial.key
wget -O /tmp/ISRG-X2.pem https://letsencrypt.org/certs/isrg-root-x2.pem
rm -f "/etc/letsencrypt/live/${hostname --fqdn}/chainZimbra.pem"
cp "/etc/letsencrypt/live/${hostname --fqdn}/chain.pem" "/etc/letsencrypt/live/${hostname --fqdn}/chainZimbra.pem"
cat /tmp/ISRG-X1.pem >> "/etc/letsencrypt/live/${hostname --fqdn}/chainZimbra.pem"
chown zimbra:zimbra /etc/letsencrypt -R
chmod 0755 /etc/letsencrypt -R
su zimbra -c '/opt/zimbra/bin/zmcertmgr deploycrt comm "/etc/letsencrypt/live/${hostname --fqdn}/cert.pem" "/etc/letsencrypt/live/${hostname --fqdn}/chainZimbra.pem"'
rm -f "/etc/letsencrypt/live/${hostname --fqdn}/chainZimbra.pem"
EOF
```

Set the correct permission, set up a cron job and run the deployment:

```
chmod +rx /usr/local/sbin/letsencrypt-zimbra
ln -s /usr/local/sbin/letsencrypt-zimbra /etc/cron.daily/letsencrypt-zimbra
/etc/cron.daily/letsencrypt-zimbra
```

Finally restart Zimbra to load the new certificate:

```
sudo su zimbra -c '/opt/zimbra/bin/zmcontrol restart'
```

The cron job will renew your certificate about 1 month prior to the expiration date, you need to manually restart Zimbra before the renewal date to load the new certificate.

Manual installation of Let's Encrypt on Zimbra

Zimbra does not ship with `ISRG Root X2` or `ISRG Root X1` so you have to provide it as a file and concatenate the chain with the root. Zimbra can work with both roots but for new deployments you will want to go with X2. Deployment of X2 or X1 is similar, just just need to download the correct root. The X1 root use is described in https://wiki.zimbra.com/index.php?title=Installing_a_LetsEncrypt_SSL_Certificate&oldid=69351 as use at your own risk as we do not support/test or update documentation for out of date deployments. Really the only thing that matters is: if you run certbot and request X1 you have to provide Zimbra X1 as well, if you request X2, Zimbra needs X2. If you run certbot without preferred-chain argument… you probably get X2 but it is recommended you make this choice consciously.

After you have received the certificate from Let's Encrypt you can deploy it on Zimbra like this:

As user root or sudo:

```
cp /etc/letsencrypt/live/barrydegraaff.nl/privkey.pem /opt/zimbra/ssl/zimbra/commercial/commercial.key
chown zimbra:zimbra /opt/zimbra/ssl/zimbra/commercial/commercial.key
wget -O /tmp/ISRG-X2.pem https://letsencrypt.org/certs/isrg-root-x2.pem
cat /tmp/ISRG-X2.pem >> /etc/letsencrypt/live/barrydegraaff.nl/chain.pem
```

As user zimbra or `sudo su zimbra -`:

```
cd ~
/opt/zimbra/bin/zmcertmgr verifycrt comm /opt/zimbra/ssl/zimbra/commercial/commercial.key /etc/letsencrypt/live/barrydegraaff.nl/cert.pem /etc/letsencrypt/live/barrydegraaff.nl/chain.pem
/opt/zimbra/bin/zmcertmgr deploycrt comm /etc/letsencrypt/live/barrydegraaff.nl/cert.pem /etc/letsencrypt/live/barrydegraaff.nl/chain.pem
```

The output should be similar to:

```
root@zimbra9:~# su zimbra -
zimbra@zimbra9:/root$ /opt/zimbra/bin/zmcertmgr verifycrt comm /opt/zimbra/ssl/zimbra/commercial/commercial.key /etc/letsencrypt/live/barrydegraaff.nl/cert.pem /etc/letsencrypt/live/barrydegraaff.nl/chain.pem
** Verifying '/etc/letsencrypt/live/barrydegraaff.nl/cert.pem' against '/opt/zimbra/ssl/zimbra/commercial/commercial.key'
Certificate '/etc/letsencrypt/live/barrydegraaff.nl/cert.pem' and private key '/opt/zimbra/ssl/zimbra/commercial/commercial.key' match.
** Verifying '/etc/letsencrypt/live/barrydegraaff.nl/cert.pem' against '/etc/letsencrypt/live/barrydegraaff.nl/chain.pem'
Valid certificate chain: /etc/letsencrypt/live/barrydegraaff.nl/cert.pem: OK
zimbra@zimbra9:/root$ cd ~
zimbra@zimbra9:~$ /opt/zimbra/bin/zmcertmgr deploycrt comm /etc/letsencrypt/live/barrydegraaff.nl/cert.pem /etc/letsencrypt/live/barrydegraaff.nl/chain.pem
** Verifying '/etc/letsencrypt/live/barrydegraaff.nl/cert.pem' against '/opt/zimbra/ssl/zimbra/commercial/commercial.key'
Certificate '/etc/letsencrypt/live/barrydegraaff.nl/cert.pem' and private key '/opt/zimbra/ssl/zimbra/commercial/commercial.key' match.
** Verifying '/etc/letsencrypt/live/barrydegraaff.nl/cert.pem' against '/etc/letsencrypt/live/barrydegraaff.nl/chain.pem'
Valid certificate chain: /etc/letsencrypt/live/barrydegraaff.nl/cert.pem: OK
** Copying '/etc/letsencrypt/live/barrydegraaff.nl/cert.pem' to '/opt/zimbra/ssl/zimbra/commercial/commercial.crt'
** Copying '/etc/letsencrypt/live/barrydegraaff.nl/chain.pem' to '/opt/zimbra/ssl/zimbra/commercial/commercial_ca.crt'
** Appending ca chain '/etc/letsencrypt/live/barrydegraaff.nl/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/lib/security/cacerts'
** NOTE: restart mailboxd to use the imported certificate.
** Saving config key 'zimbraSSLCertificate' via zmprov modifyServer zimbra9.barrydegraaff.nl...ok
** Saving config key 'zimbraSSLPrivateKey' via zmprov modifyServer zimbra9.barrydegraaff.nl...ok
** Installing imapd certificate '/opt/zimbra/conf/imapd.crt' and key '/opt/zimbra/conf/imapd.key'
** Copying '/opt/zimbra/ssl/zimbra/commercial/commercial.crt' to '/opt/zimbra/conf/imapd.crt'
** Copying '/opt/zimbra/ssl/zimbra/commercial/commercial.key' to '/opt/zimbra/conf/imapd.key'
** Creating file '/opt/zimbra/ssl/zimbra/jetty.pkcs12'
** Creating keystore '/opt/zimbra/conf/imapd.keystore'
** 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/ca.key
** Removing /opt/zimbra/conf/ca/e50a23da.0
** 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 'e50a23da.0' -> 'ca.pem'
** Creating /opt/zimbra/conf/ca/commercial_ca_1.crt
** Creating CA hash symlink '8d33f237.0' -> 'commercial_ca_1.crt'
** Creating /opt/zimbra/conf/ca/commercial_ca_2.crt
** Creating CA hash symlink '4042bcee.0' -> 'commercial_ca_2.crt'
```

Finally restart Zimbra as user zimbra or `sudo su zimbra -`:

```
zmcontrol restart
```

Using DANE

You have to use Certbot with the `--reuse-key` option, see https://blog.zimbra.com/2022/04/zimbra-skillz-enable-dane-verification-for-incoming-email-in-zimbra/

Let's Encrypt Intermediate Certificates rotating issuance

Some partners have expressed their concern with Let's Encrypt Intermediate Certificates rotating issuance as described in: https://letsencrypt.org/2024/03/19/new-intermediate-certificates

If you follow the steps in the wiki, the only thing you *pin* in the ISRG ROOT, which is the root and not an intermediate. So you will be (and have been) rotating the intermediate without any issues. This also does not affect DANE as you can *'pin'* that using the `--reuse-key` option, but that has also nothing to do with intermediates.

Using multiple https domains with SNI

Refer to: https://blog.zimbra.com/2022/06/zimbra-skillz-how-to-use-zimbra-with-multiple-https-domains-server-name-indication-sni/

Further reading

- https://techcrunch.com/2021/09/21/lets-encrypt-root-expiry

Verified Against: Zimbra Collaboration 10.1, 10.0, 9.0, 8.8	**Date Created:** 22/09/2022
Article ID: https://wiki.zimbra.com/index.php?title=Installing_a_LetsEncrypt_SSL_Certificate	**Date Modified:** 2024-09-11

Categories:

- ZCS 8.8
- Certified
- Certificates
- ZCS 10.0