

Requesting free SSL certificate

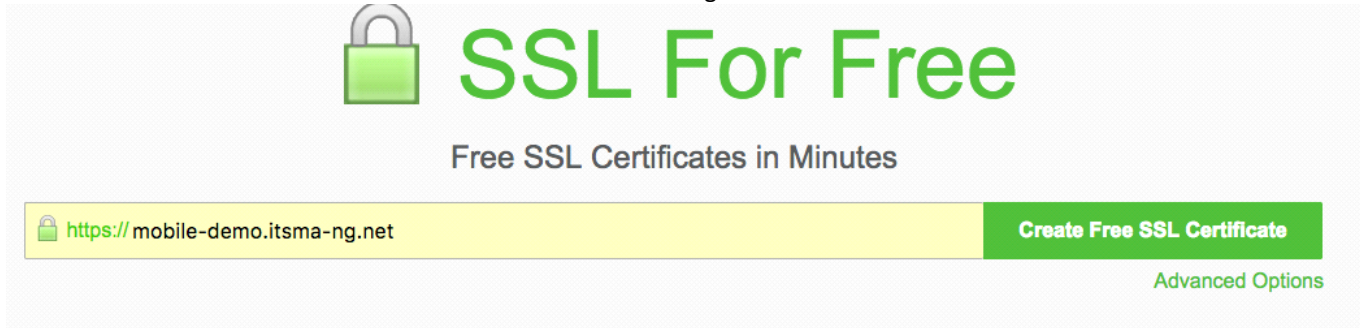
2017年10月9日 星期一 21:04

References:

- <https://www.sslforfree.com/>

Instructions

1. Go to <https://www.sslforfree.com/>
2. Enter the FQDN of the desired domain like mobile-demo.itsma-ng.net



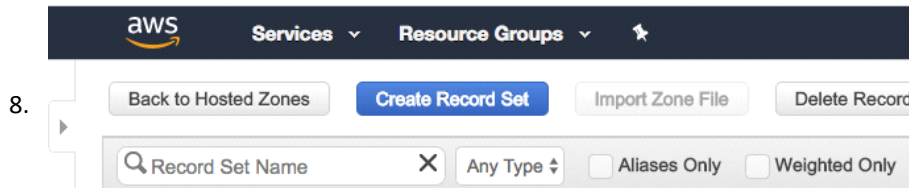
3. Click Create Free SSL Certificate
4. Select **Manual Verification (DNS)**

(Add / Edit Domains | Regenerate Account)

Verify that you own the domain through your web server or if your domain is not yet on a web server then verify it through the DNS. This prevents other people from getting an *SSL certificate* for your domain. By continuing you agree to the [Lets Encrypt service agreement](#). You may need to whitelist 66.133.109.36 if your website is behind a firewall. **If you receive a 504 Gateway timeout and cannot connect anymore then open another incognito/private browser or a different browser to connect again.** If you have your own CSR use manual verification and input it after generating domain verification files. If you use IIS on Windows you may have to do [additional steps](#).

Automatic FTP Verification Enter FTP information to automatically verify the domain	Manual Verification Upload verification files manually to your domain to verify ownership.	Manual Verification (DNS) Use this if you cannot verify through a web server or cannot use port 80. You will be adding a TXT record to your DNS server.
---	--	---

5. Click **Manual Verification**
6. In AWS Console, got to Route 53 --> Hosted Zones --> The record containing your domain
7. Click Create Record Set



9. In the form, enter the following
 - a. **Name:** you hostname in the domain name. `_acme-challenge.mobile-demo` in this example
 - b. **Type:** TXT - Text
 - c. **Value:** The generated value. `ixUfHIF1Z8bXzXRCMVCTFVfn1KsbUA7aOP1hzDX0mnE`
 - d. **TTL:** 1m

Create Record Set

Name:

Type:

Alias: ☐ Yes ☒ No

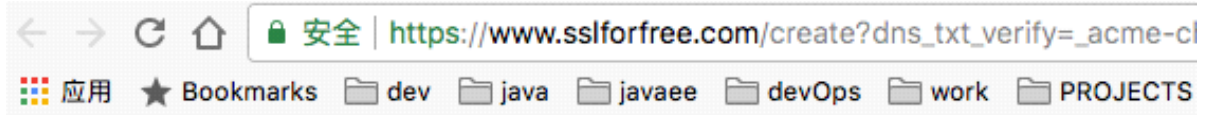
TTL (Seconds):

Value:

A text record. Enter multiple values on separate lines. Enclose text in quotation marks.
Example:
"Sample Text Entries"
"Enclose entries in quotation marks"

10.

11. Go back to the page where you get the verification information
12. Click the link at step #3 in section "Upload Verification Files"
13. You are good with the DNS verification when the response page says record found.



TXT Record Found. Make sure the value matches the value specified previous

Host: _acme-challenge.mobile-demo.itsma-ng.net

Class: IN

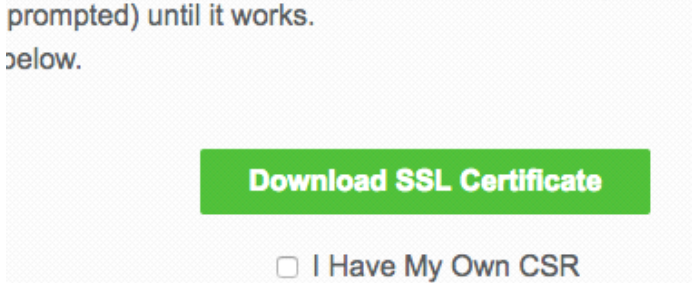
Ttl: 60

Type: TXT

Txt: ixUfHIFIZ8bXzXRCMVCTFVfnIKsbUA7aOPlhzDXOmne

Entries: ["ixUfHIFIZ8bXzXRCMVCTFVfnIKsbUA7aOPlhzDXOmne"]

14. Click the button **Download SSL Certificate** at the bottom.
Wait a couple minutes for the DNS TXT record to propagate.
If you get an error during verification that says "JWS token not prompted" until it works.
See the screenshot below.



15. Click the button below to download all files



Replace the certificate of Ingress Service

2017年8月21日 18:25

References:

- <https://docs.software.hp.com/wiki/display/ITSMA201707/Network+and+communication>

Generate free SSL certificates

- <https://www.sslforfree.com/>
- <https://letsencrypt.org/>

[Skip to end of metadata](#)

[Go to start of metadata](#)

This section provides information on network and communication security.

Replace the certificate of Ingress Service with a custom certificate

To replace the certificate and private key of Ingress Service with a custom certificate and private key, follow the steps below:

1. Generate a certificate and private key for the host on which the **Ingress Service** is running. Put the certificate and key somewhere on the master node.
2. On the master node, delete a secret with the following command:

```
kubect1 delete secret nginx-default-secret -n core
```

3. On the master node, recreate the secret with the new certificate and private key:

```
echo "
apiVersion: v1
kind: Secret
metadata:
  name: nginx-default-secret
  namespace: core
data:
  tls.crt: `base64 <certificate file name with absolute path> |tr -d \"\n\"`
  tls.key: `base64 <private key file name with absolute path> |tr -d \"\n\"`
" | kubect1 create -f -
```

4. On the master node, delete and recreate the ingress service.

```
kubect1 delete -f ${K8S_HOME}/objectdefs/nginx-ingress.yaml
kubect1 create -f ${K8S_HOME}/objectdefs/nginx-ingress.yaml
```

Replace Ingress certificate for ITSMA

1. Delete the current itsma secret named *nginx-itsma-secret* on master node
kubect1 delete secret -n itsma1 nginx-itsma-secret
2. On the master node, recreate the secret with the new certificate and private key:

```
echo "
apiVersion: v1
kind: Secret
metadata:
  name: nginx-itsma-secret
  namespace: itsma1
data:
  tls.crt: `base64 /tmp/cert.crt |tr -d \"\n\"`
  tls.key: `base64 /tmp/private.key |tr -d \"\n\"`
" | kubect1 create -f -
```

3. On the master node, delete and recreate the ingress deployment

```
kubect1 delete -f /mnt/efs/var/vols/itom/core/suite-install/itsma/output/itom-ingress-1.0.0.013/yamls/itom-nginx-ingress-deployment.yaml
kubect1 create -f /mnt/efs/var/vols/itom/core/suite-install/itsma/output/itom-ingress-1.0.0.013/yamls/itom-nginx-ingress-deployment.yaml
```