LetsEncrypt Certificates for vCenter and PSC

vCenter 6.7 is released, and you would have noticed that the default install is not working as well as expected. There's a bunch of SSL certificate errors, websockets aren't working, many strange errors.. All these things mean that you need a **valid** certificate for your vCenter (and PSC) server.

The simplest way to do this is to use AWS Route53 and acme.sh to automatically install and update LetsEncrypt certificates on your machines. This allows each machine to manage and update its SSL certificates automatically, without needing any manual intervention - which is the entire point of LetsEncrypt!

- Overview
- Route 53 Authentication
- Install acme.sh and tools
- Generate SSL Certificate for the first time
- Use 'certificate-manager' to update vCenter
- Your SSL Certificate is now valid!
- Automating Renewal
    - Create update.conf file
    - Test updater
    - Create cron job.

Overview

All of these commands are run on your vCenter (or PSC) server. The server itself will automatically renew and update DNS, without any intervention.

Route 53 Authentication

Generate IAM keys by following the AWS IAM instructions

Install acme.sh and tools

This installs the base acme.sh tool and the AWS plugin. These are hosted on our open source Git repository for your convenience, but the origin is https://github.com/Neilpang/acme.sh

```
cd ~
wget 'https://git.9r.com.au/projects/OPENSRC/repos/acme.sh/raw/acme.sh?at=refs%2Fheads%2Fmaster' -O acme.sh
chmod 755 ./acme.sh
./acme.sh --install
cd .acme.sh
wget 'https://git.9r.com.au/projects/OPENSRC/repos/acme.sh/raw/dnsapi/dns_aws.sh?at=refs%2Fheads%2Fmaster' -O
dns_aws.sh
chmod 755 ./dns_aws.sh
wget 'https://git.9r.com.au/projects/OPENSRC/repos/update-vcenter/raw/auto-updater.sh?at=refs%2Fheads%2Fmaster'
-O auto-updater.sh
chmod 755 ./auto-updater.sh
```

Generate SSL Certificate for the first time

Using the Access and Secret Keys from IAM, request a certificate for 'hostname'

```
root@vmware [ ~/.acme.sh ]# export AWS_ACCESS_KEY_ID=ABCDEFG
root@vmware [ ~/.acme.sh ]# export AWS_SECRET_ACCESS_KEY=1a2b3c4d5e6f
root@vmware [ ~/.acme.sh ]# ./acme.sh --issue --dns dns_aws -d hostname.9r.com.au
[Thu Apr 19 19:46:38 -03 2018] Registering account
[Thu Apr 19 19:46:41 -03 2018] Registered
[Thu Apr 19 19:46:41 -03 2018] ACCOUNT_THUMBPRINT='__random string here__'
[Thu Apr 19 19:46:41 -03 2018] Creating domain key
[Thu Apr 19 19:46:42 -03 2018] The domain key is here: /root/.acme.sh/hostname.9r.com.au/hostname.9r.com.au.key
[Thu Apr 19 19:46:42 -03 2018] Single domain='hostname.9r.com.au'
[Thu Apr 19 19:46:42 -03 2018] Getting domain auth token for each domain
[Thu Apr 19 19:46:42 -03 2018] Getting webroot for domain='hostname.9r.com.au'
[Thu Apr 19 19:46:42 -03 2018] Getting new-authz for domain='hostname.9r.com.au'
[Thu Apr 19 19:46:44 -03 2018] The new-authz request is ok.
[Thu Apr 19 19:46:44 -03 2018] Found domain api file: /root/acme.sh/dnsapi/dns_aws.sh
[Thu Apr 19 19:46:46 -03 2018] Geting existing records for _acme-challenge.hostname.9r.com.au
[Thu Apr 19 19:46:50 -03 2018] txt record updated success.
[Thu Apr 19 19:46:50 -03 2018] Sleep 120 seconds for the txt records to take effect
[Thu Apr 19 19:48:52 -03 2018] Verifying:hostname.9r.com.au
[Thu Apr 19 19:48:58 -03 2018] Success
[Thu Apr 19 19:48:58 -03 2018] Removing DNS records.
[Thu Apr 19 19:49:00 -03 2018] Geting existing records for _acme-challenge.hostname.9r.com.au
[Thu Apr 19 19:49:04 -03 2018] txt record deleted success.
[Thu Apr 19 19:49:04 -03 2018] Verify finished, start to sign.
[Thu Apr 19 19:49:06 -03 2018] Cert success.
-----BEGIN CERTIFICATE-----
... certificate ...
-----END CERTIFICATE-----
[Thu Apr 19 19:49:06 -03 2018] Your cert is in  /root/.acme.sh/hostname.9r.com.au/hostname.9r.com.au.cer
[Thu Apr 19 19:49:06 -03 2018] Your cert key is in  /root/.acme.sh/hostname.9r.com.au/hostname.9r.com.au.key
[Thu Apr 19 19:49:07 -03 2018] The intermediate CA cert is in  /root/.acme.sh/hostname.9r.com.au/ca.cer
[Thu Apr 19 19:49:07 -03 2018] And the full chain certs is there:  /root/.acme.sh/hostname.9r.com.au/fullchain.
cer
root@vmware [ ~/.acme.sh ]#
```

Use 'certificate-manager' to update vCenter

VMware provide 'certificate-manager' specifically for this situation

```
root@vmware [ ~/.acme.sh ]# /usr/lib/vmware-vmca/bin/certificate-manager
                _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _
               |                                                                         |
               |      *** Welcome to the vSphere 6.7 Certificate Manager  ***            |
               |                                                                         |
               |                    -- Select Operation --                               |
               |                                                                         |
               |      1. Replace Machine SSL certificate with Custom Certificate         |
               |                                                                         |
               |      2. Replace VMCA Root certificate with Custom Signing               |
               |         Certificate and replace all Certificates                        |
               |                                                                         |
               |      3. Replace Machine SSL certificate with VMCA Certificate           |
               |                                                                         |
               |      4. Regenerate a new VMCA Root Certificate and                      |
               |         replace all certificates                                        |
               |                                                                         |
               |      5. Replace Solution user certificates with                         |
               |         Custom Certificate                                              |
               |                                                                         |
               |      6. Replace Solution user certificates with VMCA certificates       |
               |                                                                         |
               |      7. Revert last performed operation by re-publishing old            |
               |         certificates                                                    |
               |                                                                         |
               |      8. Reset all Certificates                                          |
               |_ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _|
Note : Use Ctrl-D to exit.
Option[1 to 8]:
```

Select '1' and then you need to answer some questions. Note you need to provide the 'Administrator' (or equivalent) account here.

```
Note : Use Ctrl-D to exit.
Option[1 to 8]: 1

Please provide valid SSO and VC privileged user credential to perform certificate operations.
Enter username [Administrator@vsphere.local]:Administrator@vsphere.local
Enter password:

Performing operation on distributed setup, Please provide valid Infrastructure Server IP.
Server : hostname.9r.com.au
         1. Generate Certificate Signing Request(s) and Key(s) for Machine SSL certificate

         2. Import custom certificate(s) and key(s) to replace existing Machine SSL certificate

Option [1 or 2]: 2

Please provide valid custom certificate for Machine SSL.
File :
```

The files it is asking for are in the results of the 'acme.sh' command above:

```
[Thu Apr 19 19:49:06 -03 2018] Your cert is in  /root/.acme.sh/hostname.9r.com.au/hostname.9r.com.au.cer
[Thu Apr 19 19:49:06 -03 2018] Your cert key is in  /root/.acme.sh/hostname.9r.com.au/hostname.9r.com.au.key
[Thu Apr 19 19:49:07 -03 2018] The intermediate CA cert is in  /root/.acme.sh/hostname.9r.com.au/ca.cer
[Thu Apr 19 19:49:07 -03 2018] And the full chain certs is there:  /root/.acme.sh/hostname.9r.com.au/fullchain.
cer
```

Provide the new Certificate files, and continue on. It will update the required services, and then restart everything. This can take a while, depending on the size of your VM!

```
Please provide valid custom certificate for Machine SSL.
File : /root/.acme.sh/hostname.9r.com.au/hostname.9r.com.au.cer

Please provide valid custom key for Machine SSL.
File : /root/.acme.sh/hostname.9r.com.au/hostname.9r.com.au.key

Please provide the signing certificate of the Machine SSL certificate
File : /root/.acme.sh/hostname.9r.com.au/fullchain.cer

You are going to replace Machine SSL cert using custom cert
Continue operation : Option[Y/N] ? : y

Command Output: /root/.acme.sh/hostname.9r.com.au/hostname.9r.com.au.cer: OK

Get site nameCompleted [Replacing Machine SSL Cert...]
default-site-name
Lookup all services
Get service default-site-name:2f828f98-80ae-4414-8e29-8f5bc4ffeca8
Don't update service default-site-name:2f828f98-80ae-4414-8e29-8f5bc4ffeca8

 ... etc ...

Update service 345572a0-1b95-4b1e-8652-4e7e21ed251c; spec: /tmp/svcspec_renwzveb
Get service 53c2d21f-144e-4779-85ff-4cf5e180d001
Update service 53c2d21f-144e-4779-85ff-4cf5e180d001; spec: /tmp/svcspec_nutupa2h
Updated 27 service(s)
Status : 85% Completed [starting services...]

 ... this takes a while ...


Status : 100% Completed [All tasks completed successfully]

root@vmware [ ~/.acme.sh ]#
```

Your SSL Certificate is now valid!

Check that you've got a green connection, and that your wss connections are working - you can open the browser debug console and make sure you're not getting any wss errors about invalid certificates

Automating Renewal

This is the harder bit. You can't simply copy the SSL certificates around. You need to run the updater script that was downloaded at the start, which needs to know a few things

Create update.conf file

The updater script uses a file called 'update.conf' in /root/.acme.sh with the credentials required for certman.

```
root@vmware [ ~/.acme.sh ]# cat > update.conf

CERTNAME='hostname.9r.com.au'
ADMINACCOUNT='Administrator@vsphere.local'
ADMINPASS='password'
^D
root@vmware [ ~/.acme.sh ]#
```

Test updater

Run ./auto-updater.sh and it should return with no output. If it outputs something, fix it!

Create cron job.

Cron job that runs daily (at an opportune time) that will check to see if the certificate has been updated. Create this cronjob so it runs AFTER the acme.sh job, which is created at a random time.

```
root@vmware [ ~/.acme.sh ]# crontab -l
57 0 * * * "/root/.acme.sh"/acme.sh --cron --home "/root/.acme.sh" > /dev/null
root@vmware [ ~/.acme.sh ]#
```

It is also a good idea to add a 'MAILTO' field to the top of the cron file, so you will get emaied if there are any errors. An example crontab is as follows

```
MAILTO=user@example.com
57 0 * * * "/root/.acme.sh"/acme.sh --cron --home "/root/.acme.sh" > /dev/null
57 1 * * * "/root/.acme.sh"/update_vmware.sh
```