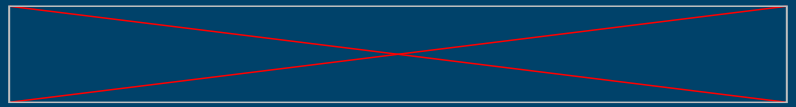
Create And Deploy Certificates on OCI web servers

Configure Apache for HTTPS (without having to pay)



We need trusted SSL certificates

- Certificates issued by a trusted authority
  - Untrusted certificates will generate warnings or errors
  - May be expensive – or free from Let's Encrypt
- Typically deployed to an internet facing web server
  - Example: Apache httpd server on an OCI compute instance
  - Production system? Deploy to a load balancer or WAF
- Often an awkward process to configure

The starting point

- An OCI compute instance running Oracle Linux
  - Absolutely normal, created from the standard image
  - Internet facing, with a public IP address
- A registered domain name
- A DNS record pointing the name to the instance IP

Software install and configuration

- Install:
  - The Extra Packages for Enterprise Linux, epel
  - Apache httpd server
  - Certbot
- Configure:
  - Virtual hosts for http :80 and https on :443
  - It works – but with a self-signed certificate

Deploy a trusted certificate

- Use the certbot utility to request a certificate
  - Run on the machine to which the name resolves
  - Let's Encrypt will create and sign a certificate
- Deployment can automatic
  - Certificate and key saved to a secure location
  - Apache configuration files updated

To conclude

- Any halfway decent website requires HTTPS
- Trusted certificates can be awkward and expensive
- Let's Encrypt is a fully functional (and free) CA
- Automation tools are now good
- The next steps:
  - Add load balancers and WAF
  - Automate certificate renewals