Getting SSL Certificates to be trusted by OpenSSL and related tools

Groundwork ships with its own copy of OpenSSL. As with every copy of OpenSSL, no certificates are installed in the trusted certificate store. If you wish OpenSSL or tools built against it to trust any certificate or CA(Certificate Authority) you will need to install them to the trusted certificate store.

Copy your certificates to /usr/local/groundwork/common/openssl/certs. If the certificates were signed by a CA(e.g., Verisign, GoDaddy, Comodo, Self-Signed CA, etc.), then the entire certificate chain must be copied here as well. Certificates must be pem formatted and have the .pem extension. Then run c_rehash:

run as root

```
/usr/local/groundwork/common/bin/c_rehash
```

This will create a symbolic link to each certificate using the hash of the certificate has the link name with a `.0` (zero) as the extension. OpenSSL and tools built against it will now recognize these certificates as trusted.

Some tools don't automatically point to the OpenSSL CADir so you might need to make further configurations to do so:

- cURL
  To get curl to work you can either use --capath at the cli or in ~/.curlrc:

  /usr/local/groundwork/users/nagios/.curlrc

  ```
  --capath /usr/local/groundwork/common/openssl/certs/
  ```

- OpenLDAP
  Groundwork has a number of OpenLDAP based tools and nagios plugins. To get these to work with ldaps add the following line to your ldap.conf and all certificates installed to OpenSSL will now be trusted:

  /usr/local/groundwork/common/etc/openldap/ldap.conf

  ```
  TLS_CACERTDIR /usr/local/groundwork/common/openssl/certs/
  ```