SSL with Solaris agent

How to use SSL with the Solaris agent:

1. Install Stunnel on Solaris.
2. Install the agent on Solaris.
3. Run the command to see the executed script:

   ```
   inetadm -l /network/uptimeagent/tcp | fgrep exec
   ```

4. Run the command to update the executed script for the agent:

   ```
   inetadm -m /network/uptimeagent/tcp exec="/usr/sbin/stunnel /usr/local/etc/stunnel/uptimeagent.conf"
   ```

   where /usr/sbin/stunnel is the path to the stunnel executable and /usr/local/etc/stunnel/uptimeagent.conf is the path to the uptimeagent.conf built for stunnel to use.
5. Run the command to see that the executed script has been changed:

   ```
   inetadm -l /network/uptimeagent/tcp | fgrep exec
   ```

6. Create the certificate that will be used by Stunnel. For example:

   ```
   openssl req -new -x509 -days 365 -nodes -config stunnel.cnf -out stunnel.pem -keyout stunnel.pem
   ```

   The following is a sample stunnel.cnf for the openssl program:

```
# create RSA certs - Server
RANDFILE = stunnel.rnd
[ req ]

default_bits = 1024
encrypt_key = yes
distinguished_name = req_dn
x509_extensions = cert_type

[ req_dn ]

countryName = Country Name (2 letter code)
countryName_default               = PL
countryName_min                    = 2
countryName_max                   = 2

stateOrProvinceName                    = State or Province Name (full name)
stateOrProvinceName_default     = Some-State

localityName                    = Locality Name (eg, city)

0.organizationName                    = Organization Name (eg, company)
0.organizationName_default      = Stunnel Developers Ltd

organizationalUnitName          = Organizational Unit Name (eg, section)
 #organizationalUnitName_default =

0.commonName                          = Common Name (FQDN of your server)
0.commonName_default            = localhost

# To create a certificate for more than one name uncomment:
# 1.commonName                  = DNS alias of your server
# 2.commonName                  = DNS alias of your server
# ... # See http://home.netscape.com/eng/security/ssl_2.0_certificate.html
# to see how Netscape understands commonName.

[ cert_type ]
nsCertType = server
```

7. Copy stunnel.pem to <stunnel install directory>/uptimeagent.pem

8. Create the uptimeagent.conf with the following lines in the stunnel install directory:

```
cert=/etc/stunnel/uptimeagent.pem
exec=/opt/uptime-agent/bin/uptimeagent
```