Dell Virtual Storage Integrator (VSI) - How to Install an Enterprise CA Signed Certificate for the Management UI

Use OpenSSL to generate a new CSR and private key

1. Create an OpenSSL configuration file (`mc-dvsi-v-202a.cnf`). Modify the highlighted variables as required.

```
# -------------- BEGIN CONFIG --------------
[ req ]
default_bits = 2048
default_keyfile = rui.key
distinguished_name = req_distinguished_name
encrypt_key = no
prompt = no
string_mask = nombstr
req_extensions = v3_req

[ v3_req ]
basicConstraints = critical,CA:false
keyUsage = digitalSignature, keyEncipherment, dataEncipherment
extendedKeyUsage = serverAuth, clientAuth
subjectAltName = @alt_names

[ alt_names ]
DNS.1 = mc-dvsi-v-202a.momusconsulting.com
DNS.2 = mc-dvsi-v-202a
IP.1 = 10.10.1.74

[ req_distinguished_name ]
countryName = GB
stateOrProvinceName = Hampshire
localityName = Basingstoke
0.organizationName = Momus Consulting
organizationalUnitName = Momus Labs
commonName = mc-dvsi-v-202a.momusconsulting.com
emailAddress = certificate-admin@momusconsulting.com

# -------------- END CONFIG --------------
```

2. From a Command Prompt, execute the OpenSSL command to create a new CSR and private key.

```
C:\Temp> openssl.exe req -sha256 -new -nodes -keyout mc-dvsi-v-202a-private-orig.key -out mc-dvsi-v-
202a.csr -config mc-dvsi-v-202a.cnf
```

3. Submit the CSR to the Enterprise Signing CA. Sign the request using the “Web Server” template or similar.

4. Save the certificate as a Base64 Encoded certificate file (`mc-dvsi-v-202a.cer`).

Apply Certificate to VSI Appliance

5. Open a SSH connection to the VSI appliance and login as root.

   NOTE: You will be required to change the default root password of "root" on first login.

```
login as: root
Keyboard-interactive authentication prompts from server:
| Password:
End of keyboard-interactive prompts from server
Last login: Thu Mar 18 14:05:53 2021 from 10.1.1.9
 14:07:25 up  4:30,  1 user,  load average: 0.00, 0.00, 0.00

91 Security notice(s)
Run 'tdnf updateinfo info' to see the details.
root@photon [ ~ ]#
```

6. Set a Hostname.

   NOTE: The prompt will change on next session login.

```
hostnamectl set-hostname mc-dvsi-v-202a.momusconsulting.com
hostnamectl status
```

```
root@photon [ ~ ]# hostnamectl set-hostname mc-dvsi-v-202a.momusconsulting.com

root@photon [ ~ ]# hostnamectl status
   Static hostname: mc-dvsi-v-202a.momusconsulting.com
         Icon name: computer-vm
           Chassis: vm
        Machine ID: c575ae8db27b4f348781356461eca3b6
           Boot ID: 57dd8492338243de892b0e4dfcfcc5a9
    Virtualization: vmware
  Operating System: VMware Photon OS/Linux
            Kernel: Linux 4.19.79-2.ph3
      Architecture: x86-64
```

7. Open the VSI IAPI Docker container

```
root@photon [ /etc/ssl/certs ]# docker exec -it iapi bash
bash-4.3#
```

8. Backup the existing UI certificate/private key.

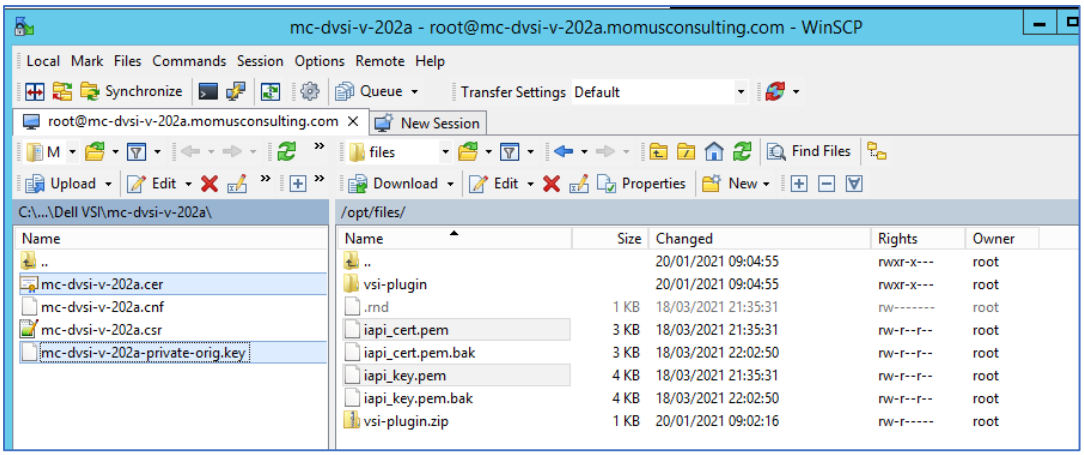
```
cd /opt/files
for file in *.pem ; do cp "$file" "$file".bak; done
```

```
bash-4.3# cd /opt/files
bash-4.3# for file in *.pem ; do cp "$file" "$file".bak; done
```

9. Open a SCP connection (WinSCP or similar) to the VSI appliance.

   - Install the Enterprise CA signed replacement certificate/private key.
   - Copy/Paste the contents of each of the following source files -> destination files & save each.

     - Signed Certificate - `mc-dvsi-v-202a.cer -> iapi_cert.pem`
     - Private Key - `mc-dvsi-v-202a-private-orig.key -> iapi_key.pem`



10. Close the VSI IAPI Docker container and restart

```
bash-4.3# exit
exit

root@photon [ ~ ]# docker restart iapi
iapi
root@photon [ ~ ]#
```

11. Reboot the VSI VM

```
root@photon [ ~ ]# reboot
```

12. Wait approx. 2 minutes for the VSI appliance to reboot and for the application to start.

13. Browse to the VSI appliance on https://{FQDN}. **Done!**