

8.1

07/25/2024 03:14:45

FAQ Article Print

Category:	i2--FAQ	Votes:	0
State:	public (all)	Result:	0.00 %
Language:	zh_CN	Last update:	20:42:37 - 04/12/2024

Keywords

8.1

Symptom (public)

```

#####
#####
1#####
#systemctl stop i2up
2#####certs
#mv /usr/info2soft/cntcenter/etc/certs
/usr/info2soft/cntcenter/etc/certs.bak
3#####certs#####
#mkdir -p /usr/info2soft/cntcenter/etc/certs
#cd /usr/info2soft/cntcenter/etc/certs

#####1#####
4#####ca#####
#openssl req -newkey rsa:3072-nodes -keyout ca.key -out ca.csr

#####
# openssl req -newkey rsa:3072-nodes -keyout ca.key -out ca.csr
Generating a RSA private key
.....+++++
.....+++++
writing new private key to 'ca.key'
Enter PEM pass phrase:#####
Verifying - Enter PEM pass phrase:
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [XX]:CN
State or Province Name (full name) []:
Locality Name (eg, city) [Default City]:
Organization Name (eg, company) [Default Company Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) []:i2#####
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:#####
An optional company name []:

5#####
# openssl x509 -req -days 365 -sha256 -extfile /etc/pki/tls/openssl.cnf
-extentions v3_ca -in ca.csr -signkey ca.key -out ca.crt

#####
# openssl x509 -req -days 365 -sha256 -extfile /etc/pki/tls/openssl.cnf
-extentions v3_ca -in ca.csr -signkey ca.key -out ca.crt
Signature ok
subject=C = CN, L = Default City, O = Default Company Ltd, CN = test-diff-name
Getting Private key
Enter pass phrase for ca.key:#####

6#####
# scp /usr/info2soft/cntcenter/etc/certs/*
ip#####:/usr/info2soft/cntcenter/etc/certs/

#####
7#####ca#####
# /usr/info2soft/cntcenter/bin/encrypt_tool pass update --ca
#####
# /usr/info2soft/cntcenter/bin/encrypt_tool pass update --ca
1.Please enter the initial password of CA Key:
*****
2.Please re-enter the initial password of CA Key:
*****

8#####
# /usr/info2soft/cntcenter/bin/encrypt_tool certs init

#####
# /usr/info2soft/cntcenter/bin/encrypt_tool certs init
validating certificate period for ca certificate
2024-04-11T20:52:12.518+0800 info [certs] Using the existing CA
certificate "/usr/info2soft/cntcenter/etc/certs/ca.crt" and key
"/usr/info2soft/cntcenter/etc/certs/ca.key"

```

```
2024-04-11T20:52:13.074+0800 info [certs] Generating "console.up.com"
certificate and key
2024-04-11T20:52:13.082+0800 info [certs] console.up.com serving cert is
signed for DNS names [localhost up.up.default up.local vm40410151922253] and
IPs [127.0.0.1 ::1 10.1.7.99]
2024-04-11T20:52:13.947+0800 info [certs] Generating "db" certificate
and key
2024-04-11T20:52:13.954+0800 info [certs] db serving cert is signed for
DNS names [localhost up.up.default up.local vm40410151922253] and IPs
[127.0.0.1 ::1 10.1.7.99]
2024-04-11T20:52:13.954+0800 info [certs] Valid certificates and keys
now exist in "/usr/info2soft/cntlcenter/etc/certs/"
2024-04-11T20:52:14.960+0800 info [certs] Generating "st" key and public
key
9#####lic.crt#####certs
#cp /usr/info2soft/cntlcenter/etc/certs.bak/lic.crt
/usr/info2soft/cntlcenter/etc/certs/
10#####
#chown i2runner. /usr/info2soft/cntlcenter/etc/certs/ -R

11#####i2up
#systemctl start i2up
12#####
#####
13#####

14#####
#####1#####1
#####

2#####2#####
#mkdir -p /usr/info2soft/cntlcenter/
3#####1 #####etc#####2#
#scp -r /usr/info2soft/cntlcenter/etc/ ip://usr/info2soft/cntlcenter/

4#####2
```

Problem (public)

Solution (public)