Enroll Fabric admin

Run the following command to copy the Amazon Managed Blockchain TLS certificate chain to your Fabric client. This allows your client to recognize valid certificates within your blockchain network and generate additional certificates for your member organization.

```
aws s3 cp s3://$AWS_DEFAULT_REGION.managedblockchain/etc/managedblockchain-tls-chain.pem ~/managedblockchain-tls-chain.pem
```

Then run the following to test that you successfully copied the file.

```
openssl x509 -noout -text -in ~/managedblockchain-tls-chain.pem
```

It should display human-readable information about the certificate, looking something like this:

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            36\:a8:96:2d:7f:12:48:5e:84\:d0:70:13\:d7:7d:3f:9b
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=US, ST=WA, L=Seattle, O=Amazon Web Services, Inc., OU=Amazon Managed Blockchain, CN=Amazon Managed Blockchain us-east
        Validity
            Not Before: Apr 30 08:48:13 2019 GMT
            Not After : Apr 25 08:48:13 2034 GMT
        Subject: C=US, ST=WA, L=Seattle, O=Amazon Web Services, Inc., OU=Amazon Managed Blockchain, CN=Amazon Managed Blockchain us-eas
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (4096 bit)
                Modulus:
                    00\:d8:9a:9a:37\:ee:02:79\:ab:57\:fa:1a:00\:b4\:c9:
                    8e:67:8c:30\:e0\:dc:25:8f\:aa:6d\:f3:09\:bc:8d:5c:
                    a8\:b2\:ef:64:3d\:c8:7e:0d:45:2b:09\:cc:1e:8d\:f0:
                    d7:88:7d:13:6f:3e:8f\:e4:21:03\:b2\:ff:5d:0f\:eb:
                    8b:51:01\:e6:11:07:2f\:c7:88:56\:d9:89:07:98:75:
                    42\:ac:02:54:90:13:82\:ac\:cc:67:83:0b\:eb\:f4:52:
                    55:22\:d5:22:39\:b9:3f:08:90\:b2:08\:a2:84\:ec:44:
                    ba\:ff:2f:1c:56:13:96:94\:fa:45:70:53\:ac:8a:88:
                    1c:18:7e:34:75\:d1:05:2e\:ba\:aa\:c8:73\:f8:82\:dd:
                    0b:02\:bb:4e:09:42\:bf:6d\:d7:60:38\:a4:16:52:3a:
                    80\:c7:4f:3a\:b8\:bf:6a:2d\:bf\:ee:14:1c:0f\:c9:33:
                    d7:5e:10\:f9:1d:0c\:c8\:f9\:bf:73\:d2\:a9\:be:74:22:
                    30\:dc\:be:08:74:96\:c7:8d:6f:50:52:0f:32:2a\:b5:
                    91:2c:29:6a\:c3\:ab\:ab:73\:d5:61:7b\:bd\:d1:6e\:d1:
                    f6:8d\:bf:7a:4c\:b7:9b\:cd\:d2:2c:3b\:ca:48:02:6f:
                    02:3d:0c:0e:72:17:18\:f7:55\:d3:5b:35:52\:e9:47:
```

```
                    03\:de:45:96:73:67:63:13:06:3b:0d:91\:a4:5d\:f5:
                    1a:23:57:8d:84\:ca:98:6c:81\:b8:15\:d7\:f9\:b3:19:
                    0a:37\:ac:8f:89:7c:1b:72\:e3\:bb:1f:05\:fc\:ab:27:
                    cf\:ee\:d6:3a:70:36\:e4:3f:3a\:ec\:ee\:a2:2e:7d:98:
                    8f\:c7\:c3:92:57:18:8f:69\:f2\:d6:9e:28\:b4\:e3:6a:
                    6b:5c:2d\:d1:18:4f:64:4e:86:4e\:b8:6d:34\:e5:47:
                    41:4e:9e:37:96:01:3e:60:53\:cf\:d5:65\:c8:04\:ac:
                    f5:69:05:55\:d5:97:06\:b6:27\:bb:57\:f5:0d:35\:bc:
                    bc:20:32\:ed\:fc:9e:5d:25\:cb:13\:ee\:e1:0f\:dd:07:
                    30:31:6c\:b4:15\:b3:97:3b\:b8\:b2\:dd\:b9\:ef:24:8f:
                    01\:d8:8c\:e9\:dd\:ea\:d5\:db:24:97:41:08:4b:1d:77:
                    eb\:a9:16\:ac:79\:fd\:b3:51:30:83:03\:cc\:c3:6f:08:
                    5b:74:6c:74:9f\:d7\:e9\:c1:4e:26:19:4e\:ed:36:46:
                    b6\:f4:09:88:87\:ce\:f5:6d\:a7:9d\:ad:60:03:23:80:
                    09\:e1\:b0\:af:2b\:f4:7f:43:56\:c9:7a:51:79:7e:2c:
                    bd:74:80:9d\:e3:49:93\:fd:5d:9f:2e\:b1\:c4:79:2b:
                    ab\:ce:08\:f4:19:8a:72:3c\:c6:73:90:4d:0f:07:9f:
                    c2:54:3a\:a3:9b:30:99:73:01:2c\:f2:25:72\:ea:7f:
                    ed:02:4b
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints: critical
                CA\:TRUE
            X509v3 Subject Key Identifier:
                87\:B6\:B1:92\:DE:87\:B4\:C8\:AB\:F2\:ED:23\:D5\:B1:9C\:E6:18:94:27\:E8
    Signature Algorithm: sha256WithRSAEncryption
         3b\:aa:64\:fd:6a\:bd:1e\:b9:59:93\:ed:49\:c1:06\:ee:0c:88\:cf:
         c4\:b6\:d7:7d\:f7\:c1\:e7:77\:f1:8e:3d\:c9:29\:da:09:0e\:cc\:a1:
         16\:f2\:e7:20:1b\:df:6f:89:2a\:ca\:a5:95\:e2:09:5c\:f5:88:3d:
         bf:82\:be:1e:45\:bc:9d\:ff:1e:43:76\:e3:06:98:47:0e\:c5:15:
         2d\:a8:13\:e9:10:32\:f3\:b9:19\:a9\:d9:7a:90:4b:28\:e3:01:80:
         01:1f\:b8:6c\:b1\:a4:92\:e4:71\:b1\:bb:8f\:c3\:ec:87\:de\:c8:2b:
         5d\:b5:09:30:90:5b:18\:d9:75:5e:1b:37:7b:68:73\:db:2f\:ca:
         3e\:c5:47:2f:2e:35:1f:0d:6a\:e9:9c\:e8\:c8\:aa:8a:79\:ad:9f:
         87:6e:64\:f8\:b1:9e:53:21:40\:e4\:a5:91:6b\:a3\:b3\:eb\:a4\:e4:
         7c:55:03\:e6\:dc:71\:e9:4b:88\:ff\:e8\:af:57\:f6:91\:bb:18:5d:
         43\:cb\:f9\:e5\:f4:85:9f\:a1:3d:88\:a8:62\:cd\:b8:33:0c\:d2\:c2:
         39:82\:b7:7b\:b2:60:33:97:09\:f1\:c3\:f1:52:43\:be:8f:66:89:
         16\:e5:12:28:0d\:eb\:d1:79:90\:d6\:c8\:c3:4c:8d\:ea:96:9b\:c6:
         13:81:11:81:58\:a6:27:7d\:fb:50:3f:66:74\:ef:5a\:b8\:f3:90:
         22\:cc:88\:c1
```

Enroll the client as a Fabric admin by using the member admin credentials we created earlier.

```
cd
fabric-ca-client enroll -u https://$MEMBER_ADMIN\:Admin123@$CASERVICEENDPOINT --tls.certfiles ~/managedblockchain-tls-chain.pem -M admin
cp -r ~/admin-msp/signcerts ~/admin-msp/admincerts
```

If all goes well, you should see output like this:

```
2020/05/11 03:29:46 [INFO] TLS Enabled
2020/05/11 03:29:46 [INFO] generating key: &{A\:ecdsa S:256}
2020/05/11 03:29:46 [INFO] encoded CSR
2020/05/11 03:29:47 [INFO] Stored client certificate at $HOME/admin-msp/signcerts/cert.pem
2020/05/11 03:29:47 [INFO] Stored root CA certificate at $HOME/admin-msp/cacerts/ca-m-m7medjz3ajcqlaoy6tjhs3dl7a-n-vjetdnyjunaofccqhjr6i
```

In Hyperledger Fabric, the Membership Service Provider (MSP) identifies which root CAs and intermediate CAs are trusted to define the members of a trust domain. Certificates for the administrator's MSP are in `$FABRIC_CA_CLIENT_HOME`, which is `~/admin-msp` in this workshop.

> It may take a minute or two after you enroll for you to be able to use your administrator certificate for Fabric operations. This delay is due to the time it takes for Amazon Managed Blockchain to copy the new certificate to your peer nodes so that they recognize it. This is one of the many tasks that is managed for you by AWS.

Previous Next