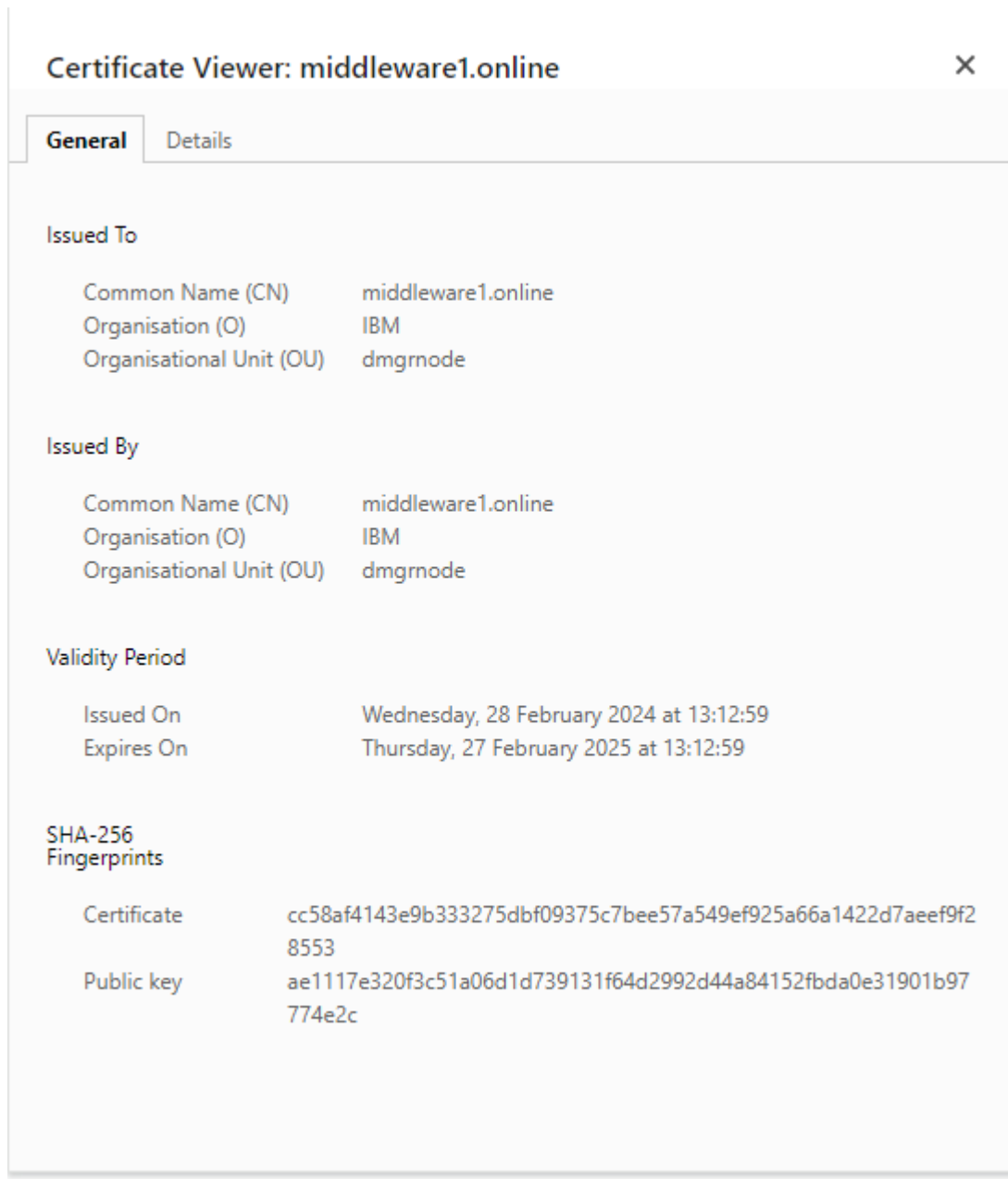


SSL Renewal in WAS with Self Signed certificates

I am renewing cell default certificate which came along with default installation.

Start all services and check the default certificate

Log on to console and check current certificate details



Navigate to till Cell location and take backup of key.p12,trust.p12 and security.xml

```
drwxr-xr-x 9 wasadmin2 wasadmin2 142 Mar 9 12:02 blas
-rwxr-xr-x 1 wasadmin2 wasadmin2 960 Mar 9 17:49 cell.xml
-rwxr-xr-x 1 wasadmin2 wasadmin2 389 Mar 9 18:13 multibroker.xml
drwxr-xr-x 3 wasadmin2 wasadmin2 23 Mar 9 18:13 clusters
-rw-r--r-- 1 wasadmin2 wasadmin2 307 Mar 12 20:38 xdcatalognodes.config
-rw-r--r-- 1 wasadmin2 wasadmin2 400 Mar 12 20:38 overlaynodes.config
-rwxr-xr-x 1 wasadmin2 wasadmin2 4274 Mar 12 20:55 key.p12_backup
-rwxr-xr-x 1 wasadmin2 wasadmin2 1430 Mar 12 20:56 trust.p12_backup
-rwxr-xr-x 1 wasadmin2 wasadmin2 50391 Mar 12 20:56 security.xml_backup
wasadmin2@middleware1[20:56:19]:/opt/wasadmin2/AppServer/profiles/dmgr/config/cells/Cell01$
```

Copy these p12 to different location in /tmp/ssl-renewal

```
wasadmin2@middleware1[21:36:24]:/home/wasadmin2$cd /tmp/ssl-renewal/
wasadmin2@middleware1[21:36:36]:/tmp/ssl-renewal$pwd
/tmp/ssl-renewal
wasadmin2@middleware1[21:36:39]:/tmp/ssl-renewal$ls -ltr
total 12
-rwxr-xr-x 1 wasadmin2 wasadmin2 4274 Mar 12 20:58 key.p12
-rwxr-xr-x 1 wasadmin2 wasadmin2 1430 Mar 12 20:58 trust.p12
wasadmin2@middleware1[21:36:40]:/tmp/ssl-renewal$
```

List the certificated in keystore

gskcmd -cert -list -db key.p12 -pw WebAS

```
wasadmin2@middleware1[10:10:41]:/tmp/ssl-renewal$gskcmd -cert -list -db key.p12 -pw WebAS
Certificates in database /tmp/ssl-renewal/key.p12:
default
wasadmin2@middleware1[10:11:31]:/tmp/ssl-renewal$
```

Check the details of the certificate

gskcmd -cert -details -label default -db key.p12 -pw WebAS

```
wasadmin2@middleware1[10:11:31]:/tmp/ssl-renewal$gskcmd -cert -details -label default -db key.p12 -pw WebAS
Label: default
Key Size: 2048
Version: X509 V3
Serial Number: 03 BE 41 41 17 B7
Issued by: CN=middleware1.online, OU=Root Certificate, OU=Cell01, OU=dmgrnode, O=IBM, C=US
Subject: CN=middleware1.online, OU=Cell01, OU=dmgrnode, O=IBM, C=US
Valid: From: Wednesday, February 28, 2024 1:12:59 PM IST To: Thursday, February 27, 2025 1:12:59 PM IST
Fingerprint:
SHA1: 7A:13:5C:D7:19:8A:44:0F:40:2A:37:2F:3A:D9:56:FE:51:86:BA:C8
SHA256: CC:58:AF:41:43:E9:B3:33:27:5D:BF:09:37:5C:7B:EE:57:A5:49:EF:92:5A:66:A1:42:2D:7A:EE:F9:F2:85:53
HPKP: rhEX4yDzxRoG0dc5Ex9k0pktrKhBUvvaDjGQ65d3Tiw=

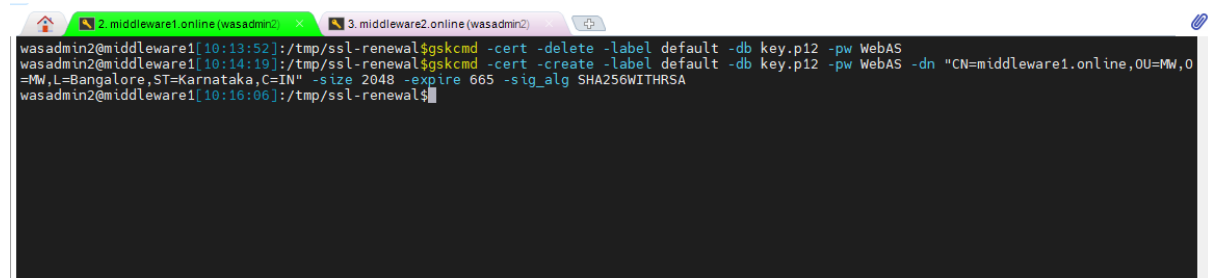
Extensions:
- AuthorityKeyIdentifier: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KeyIdentifier [
0000: 45 86 4e 0c 79 29 31 46
]
]
- SubjectKeyIdentifier: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 4a 9b 8d 9e 76 a4 33 ef
]
]
- ExtKeyUsage: serverAuth, clientAuth
- SAN: ObjectId: 2.5.29.17 Criticality=false
SubjectAlternativeName [
[RFC822Name: ProfileUUID:dmgr-DEPLOYMENT_MANAGER-4c857bc4-a351-4785-8da1-65d99f8a9a30, DNSName: middleware1.online]]
Signature Algorithm: SHA256withRSA (1.2.840.113549.1.1.11)
Trust Status: enabled
```

Delete old certificate

gskcmd -cert -delete -label default -db key.p12 -pw WebAS

Create New self-signed certificate

gskcmd -cert -create -label default -db key.p12 -pw WebAS -dn "CN=middleware1.online,OU=MW,O=MW,L=Bangalore,ST=Karnataka,C=IN" -size 2048 -expire 665 -sig_alg SHA256WITHRSA



```
wasadmin2@middleware1[10:13:52]:/tmp/ssl-renewal$gskcmd -cert -delete -label default -db key.p12 -pw WebAS
wasadmin2@middleware1[10:14:19]:/tmp/ssl-renewal$gskcmd -cert -create -label default -db key.p12 -pw WebAS -dn "CN=middleware1.online,OU=MW,O=MW,L=Bangalore,ST=Karnataka,C=IN" -size 2048 -expire 665 -sig_alg SHA256WITHRSA
wasadmin2@middleware1[10:16:06]:/tmp/ssl-renewal$
```

Check the certificate details

```
wasadmin2@middleware1[10:16:06]:/tmp/ssl-renewal$gskcmd -cert -details -label default -db key.p12 -pw WebAS
Label: default
Key Size: 2048
Version: X509 V3
Serial Number: 65 F1 2F 8D
Issued by: CN=middleware1.online, OU=MW, O=MW, L=Bangalore, ST=Karnataka, C=IN
Subject: CN=middleware1.online, OU=MW, O=MW, L=Bangalore, ST=Karnataka, C=IN
Valid: From: Wednesday, March 13, 2024 10:16:05 AM IST To: Wednesday, January 7, 2026 10:16:05 AM IST
Fingerprint:
  SHA1: 85:15:E7:4F:89:83:BA:85:91:1A:C6:B2:58:9C:7C:AA:BA:6E:31:AB
  SHA256: E4:17:40:7D:95:4A:B8:FA:E5:45:61:CA:D0:6C:A8:9D:04:BA:01:40:95:51:DC:5C:7F:5F:F6:9C:B0:70:2A:B8
  HPKP: WoVI41f0h8/EKhYTLVHhk514S9f3mohvKk4Gug2maZE=

Extensions:
  - AuthorityKeyIdentifier: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
  KeyIdentifier [
    0000: 32 dc 95 77 44 3d 64 18 6c 8f e8 2c aa cd 2d 9e 2..wD.d.l.....
    0010: 0f 43 cd 12 .C..
  ]
]

  - SubjectKeyIdentifier: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
  KeyIdentifier [
    0000: 32 dc 95 77 44 3d 64 18 6c 8f e8 2c aa cd 2d 9e 2..wD.d.l.....
    0010: 0f 43 cd 12 .C..
  ]
]

Signature Algorithm: SHA256withRSA (1.2.840.113549.1.1.11)
Trust Status: enabled
wasadmin2@middleware1[10:19:44]:/tmp/ssl-renewal$
```

Extract the Certificate and add to trust.p12

gskcmd -cert -extract -label default -db key.p12 -pw WebAS -format ascii -target key.cer

```
2. middleware1.online (wasadmin2) 3. middleware2.online (wasadmin2)
wasadmin2@middleware1[10:19:44]:/tmp/ssl-renewal$gskcmd -cert -extract -label default -db key.p12 -pw WebAS -format ascii -target key.cer
wasadmin2@middleware1[10:21:39]:/tmp/ssl-renewal$ls -ltr
total 12
-rwxr-xr-x 1 wasadmin2 wasadmin2 1430 Mar 12 20:58 trust.p12
-rwxr-xr-x 1 wasadmin2 wasadmin2 3794 Mar 13 10:16 key.p12
-rw-r--r-- 1 wasadmin2 wasadmin2 1320 Mar 13 10:21 key.cer
wasadmin2@middleware1[10:21:41]:/tmp/ssl-renewal$
```

gskcmd -cert -add -label default -db trust.p12 -pw WebAS -file key.cer

```
2. middleware1.online (wasadmin2) 3. middleware2.online (wasadmin2)
wasadmin2@middleware1[10:19:44]:/tmp/ssl-renewal$gskcmd -cert -extract -label default -db key.p12 -pw WebAS -format ascii -target key.cer
wasadmin2@middleware1[10:21:39]:/tmp/ssl-renewal$ls -ltr
total 12
-rwxr-xr-x 1 wasadmin2 wasadmin2 1430 Mar 12 20:58 trust.p12
-rwxr-xr-x 1 wasadmin2 wasadmin2 3794 Mar 13 10:16 key.p12
-rw-r--r-- 1 wasadmin2 wasadmin2 1320 Mar 13 10:21 key.cer
wasadmin2@middleware1[10:21:41]:/tmp/ssl-renewal$gskcmd -cert -add -label default -db trust.p12 -pw WebAS -file key.cer
wasadmin2@middleware1[10:24:31]:/tmp/ssl-renewal$
```

Check the certificate in trust.p12

```
wasadmin2@middleware1[10:25:46]:/tmp/ssl-renewal$gskcmd -cert -list -db trust.p12 -pw WebAS
Certificates in database /tmp/ssl-renewal/trust.p12:
default
root
wasadmin2@middleware1[10:25:49]:/tmp/ssl-renewal$
```

Copy both p12 file to cell location and synchronize.

```
wasadmin2@middleware1[10:25:46]:/tmp/ssl-renewal$gskcmd -cert -list -db trust.p12 -pw WebAS
Certificates in database /tmp/ssl-renewal/trust.p12:
default
root
wasadmin2@middleware1[10:25:49]:/tmp/ssl-renewal$dmgr
wasadmin2@middleware1[10:26:58]:/opt/wasadmin2/AppServer/profiles/dmgr$cp /tmp/ssl-renewal/*.p12 ./config/cells/Cell01/
wasadmin2@middleware1[10:27:23]:/opt/wasadmin2/AppServer/profiles/dmgr$ls -ltr ./config/cells/Cell01/*.p12
-rwxr-xr-x 1 wasadmin2 wasadmin2 4242 Feb 29 13:13 ./config/cells/Cell01/rsatoken-key.p12
-rwxr-xr-x 1 wasadmin2 wasadmin2 1430 Feb 29 13:13 ./config/cells/Cell01/rsatoken-trust.p12
-rwxr-xr-x 1 wasadmin2 wasadmin2 3794 Mar 13 10:27 ./config/cells/Cell01/key.p12
-rwxr-xr-x 1 wasadmin2 wasadmin2 2518 Mar 13 10:27 ./config/cells/Cell01/trust.p12
wasadmin2@middleware1[10:27:45]:/opt/wasadmin2/AppServer/profiles/dmgr$
```

The screenshot shows the IBM WebSphere Administrative Console interface. On the left is a navigation tree with categories like Core Groups, Applications, Jobs, Services, Resources, Runtime Operations, Security, Operational policies, Environment, and System administration. The main panel displays the 'Nodes' page for 'Cell=Cell01, Profile=dmgr'. It includes a 'Nodes' section with a description, a 'Preferences' section with buttons for 'Add Node', 'Remove Node', 'Force Delete', 'Synchronize', 'Full Resynchronize', and 'Stop', and a table of nodes.

Select	Name	Host Name	Version	Discovery Protocol	Status
<input checked="" type="checkbox"/>	dmgrnode	middleware1.online	ND 9.0.5.16	TCP	Managed
<input type="checkbox"/>	middleware1	middleware1.online	ND 9.0.5.16	TCP	Managed
<input type="checkbox"/>	middleware2	middleware2.online	ND 9.0.5.16	TCP	Managed
Total 3					

Kill dmgr and restart

Log into console and check the current certificate

Restart all Nodeagents and jvms and try to access the applications from Webserver

```
wasadmin2@middleware1[10:37:24]:/opt/wasadmin2/AppServer/profiles/amg:~$  
wasadmin2@middleware1[10:37:24]:/home/wasadmin2$stopServer.sh server1 ; stopNode.sh ; startNode.sh ; startServer.sh server1  
ADMU0116I: Tool information is being logged in file  
/opt/wasadmin2/AppServer/profiles/base/logs/server1/stopServer.log  
ADMU0128I: Starting tool with the base profile  
ADMU3100I: Reading configuration for server: server1  
ADMU3201I: Server stop request issued. Waiting for stop status.
```

WebSphere Integrated Solution x Table Lister x +

← → ↻ ⚙️ middlewareweb.online/hrlistner/listtable

🌐 New Tab

In ListTable Servlet
In getJNDIConnection Opened connection to Oracle
Listing Tables...

Table Name
LOGMNR_SESSION_EVOLVES
LOGMNR_GLOBALS
LOGMNR_GT_TAB_INCLUDES
LOGMNR_GT_USER_INCLUDES
LOGMNR_GT_XID_INCLUDES
LOGMNR_PDB_INFOS
LOGMNR_DIDS
LOGMNR_UIDS
LOGMNRGGC_GTLO
LOGMNRGGC_GTCS
LOGMNR_DBNAME_UID_MAP
LOGMNR_LOGS
LOGMNR_PROCESSED_LOGS
LOGMNR_SPILLS
LOGMNR_AGE_SPILLS
LOGMNR_RESTART_CKPT_TXINFOS
LOGMNR_ERRORS
LOGMNR_RESTART_CKPTS
LOGMNR_FILTERS
LOGMNR_SESSION_ACTIONS\$
LOGMNR_PARAMETERS
LOGMNR_SESSIONS
LOGMNR_PROFILE_TABLE_STAT\$
LOGMNR_PROFILE_PLSQL_STAT\$
LOGMNR_MDDL\$
REDO_DB
REDO_LOG
ROLLING\$CONNECTIONS
ROLLING\$DATABASES
ROLLING\$DIRECTIVES