

Konfigurieren des Zertifikats für FND für die SSM-Kommunikation

Inhalt

[Einführung](#)

[Problem](#)

[Lösung](#)

Einführung

In diesem Dokument wird beschrieben, wie Kommunikationsfehler zwischen Field Network Director (FND) und Software Security Module (SSM) richtig konfiguriert werden.

Problem

Seit FND 4.4 erfordert die Kommunikation zwischen dem FND-Anwendungsserver und dem SSM-Dienst eine gegenseitige Authentifizierung.

Falls diese gegenseitige Authentifizierung nicht richtig konfiguriert ist oder die Zertifikate nicht übereinstimmen, wird die Verbindung von FND zum SSM verweigert.

Dies wird in **server.log** angezeigt, wenn die Protokollierung auf debug festgelegt ist, wie folgt:

```
7645: SLC-FND: Jun 20 2019 13:22:49.929 +0000: %IOTFND-7-UNSPECIFIED:
%[ch=SSMClient][sev=DEBUG][tid=http-/0.0.0.0:443-5]: Sending request to SSM Server. Request
:https://127.0.0.1:8445/api/v0/ssmws/loadKeyStore.json
7646: SLC-FND: Jun 20 2019 13:22:49.930 +0000: %IOTFND-7-UNSPECIFIED:
%[ch=BasicClientConnectionManager][sev=DEBUG][tid=http-/0.0.0.0:443-5]: Get connection for route
{s}->https://127.0.0.1:8445
7647: SLC-FND: Jun 20 2019 13:22:49.931 +0000: %IOTFND-7-UNSPECIFIED:
%[ch=DefaultClientConnectionOperator][sev=DEBUG][tid=http-/0.0.0.0:443-5]: Connecting to
127.0.0.1:8445
7648: SLC-FND: Jun 20 2019 13:22:49.938 +0000: %IOTFND-7-UNSPECIFIED:
%[ch=DefaultClientConnection][sev=DEBUG][tid=http-/0.0.0.0:443-5]: Connection
org.apache.http.impl.conn.DefaultClientConnection@370804ff closed
7649: SLC-FND: Jun 20 2019 13:22:49.938 +0000: %IOTFND-7-UNSPECIFIED:
%[ch=DefaultClientConnection][sev=DEBUG][tid=http-/0.0.0.0:443-5]: Connection
org.apache.http.impl.conn.DefaultClientConnection@370804ff shut down
7650: SLC-FND: Jun 20 2019 13:22:49.938 +0000: %IOTFND-7-UNSPECIFIED:
%[ch=BasicClientConnectionManager][sev=DEBUG][tid=http-/0.0.0.0:443-5]: Releasing connection
org.apache.http.impl.conn.ManagedClientConnectionImpl@7bc2e02f
7651: SLC-FND: Jun 20 2019 13:22:49.938 +0000: %IOTFND-7-UNSPECIFIED:
%[ch=BasicClientConnectionManager][sev=DEBUG][tid=http-/0.0.0.0:443-5]: Connection can be kept
alive for 9223372036854775807 MILLISECONDS
7652: SLC-FND: Jun 20 2019 13:22:49.938 +0000: %IOTFND-7-UNSPECIFIED:
%[ch=SSMClient][sev=DEBUG][tid=http-/0.0.0.0:443-5][part=7652.1/114]: Please verify SSM server
status. No response received.
7653: SLC-FND: Jun 20 2019 13:22:49.938 +0000: %IOTFND-7-UNSPECIFIED:
%[ch=SSMClient][sev=DEBUG][tid=http-/0.0.0.0:443-5][part=7652.2/114]:
javax.net.ssl.SSLPeerUnverifiedException: peer not authenticated
```



```
4aUEdBZxv29+QQ7dq6ZZOXQ=
-----END CERTIFICATE-----
```

3. Führen Sie diesen Befehl aus, um das Zertifikat als vertrauenswürdig im `ssm_web_keystore` zu importieren:

```
[root@fndnms ~]# keytool -import -trustcacerts -alias fnd -keystore /opt/cgms-
ssm/conf/ssm_web_keystore -file /opt/cgms/server/cgms/conf/webcert.crt
Enter keystore password:
Owner: CN=CG-NMS, OU=IoTSSG, O=Cisco Systems, L=San Jose, ST=CA, C=US
Issuer: CN=CG-NMS, OU=IoTSSG, O=Cisco Systems, L=San Jose, ST=CA, C=US
Serial number: 1122fead
Valid from: Tue Mar 03 22:58:13 CET 2015 until: Sun Mar 01 22:58:13 CET 2020
Certificate fingerprints:
    MD5: 6D:63:B9:8B:3F:C5:E9:6B:2B:DD:77:30:55:9D:C6:E7
    SHA1: 5F:3B:84:92:06:22:CE:C4:FA:8B:F0:46:65:4B:CE:74:61:AA:3B:AE
    SHA256:
1C:59:50:40:92:09:66:D3:67:E9:AE:CA:6D:C8:25:88:FF:A8:26:F7:62:8A:13:EB:0E:EC:57:32:DB:03:94:31
    Signature algorithm name: SHA256withRSA
    Version: 3
```

Extensions:

```
#1: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 7F 21 68 0E 3D 21 24 BB 54 BB A6 6D 28 21 EE 8A .!h.=!$.T..m(!..
0010: C0 90 7E 5E ...^
]
]
```

```
Trust this certificate? [no]: yes
Certificate was added to keystore
```

4. Starten Sie nach dem Importieren des Zertifikats den SSM-Dienst neu:

```
[root@fndnms ~]# systemctl restart ssm
[root@fndnms ~]# systemctl status ssm
ssm.service - (null)
   Loaded: loaded (/etc/rc.d/init.d/ssm; bad; vendor preset: disabled)
   Active: active (running) since Thu 2019-06-20 17:44:11 CEST; 5s ago
     Docs: man:systemd-sysv-generator(8)
  Process: 11463 ExecStop=/etc/rc.d/init.d/ssm stop (code=exited, status=0/SUCCESS)
  Process: 11477 ExecStart=/etc/rc.d/init.d/ssm start (code=exited, status=0/SUCCESS)
   CGroup: /system.slice/ssm.service
           11485 java -server -Xms128m -Xmx1g -XX:MaxPermSize=256m -server -
XX:+HeapDumpOnOutOfMemoryError -XX:HeapDumpPath=/opt/cgms-ssm/log -XX:-OmitStackTraceInFastThrow
-Dbase.dir=/opt/cgms-ssm -Dlog4j...

Jun 20 17:44:10 fndnms systemd[1]: Starting (null)...
Jun 20 17:44:11 fndnms ssm[11477]: Starting Software Security Module Server: [ OK ]
Jun 20 17:44:11 fndnms systemd[1]: Started (null).
```

Sie können überprüfen, ob FND mit SSM kommunizieren kann. Navigieren Sie in der FND-GUI zu **Admin > Certificates > Certificate for CSMP**.

Wenn alles gut geht, sollten Sie das CSMP-Zertifikat in SSM sehen können, wie im Bild gezeigt.



Certificate:

Data:

```
Version: 3
Serial Number: 1911174027
Signature Algorithm: SHA256withECDSA
Issuer: CN=SSM_CSMP, OU=CENBU, O=Cisco, L=San Jose, ST=CA, C=US
Validity
  Not Before: Tue Jul 22 23:32:52 UTC 2014
  Not After : Thu Jul 21 23:32:52 UTC 2044
Subject: CN=SSM_CSMP, OU=CENBU, O=Cisco, L=San Jose, ST=CA, C=US
Fingerprints:
MD5: 2E:AC:06:1F:3E:AB:A6:BE:33:1F:1E:EF:33:D9:80:29
SHA1: 48:A2:EC:63:2F:6F:54:25:23:5D:E7:6F:4E:E9:8E:2D:93:50:A0:FF
Subject Public Key Info:
  Public Key Algorithm: EC
    30:59:30:13:06:07:2A:86:48:CE:3D:02:01:06:08:
    2A:86:48:CE:3D:03:01:07:03:42:00:04:23:D2:83:
    45:E8:D5:DF:86:9D:6E:E7:58:0D:C1:8F:35:9D:57:
    B1:3D:50:4A:16:01:15:C4:81:19:B0:E6:60:B8:64:
    14:01:5D:56:83:BE:E1:85:98:CB:90:E1:F7:9B:F4:
    33:5A:4B:29:AD:35:69:9B:4F:DC:42:7F:EB:C2:99:
    A5
X509v3 extensions:
```

- Binary
- Base64

Download