Configura certificato per FND alla comunicazione SSM

Sommario

Introduzione

Questo documento descrive come configurare correttamente i problemi di comunicazione tra Field Network Director (FND) e Software Security Module (SSM).

Problema

A partire da FND 4.4, la comunicazione tra il server applicazioni FND e il servizio SSM richiede l'autenticazione reciproca.

Se l'autenticazione reciproca non è configurata correttamente o i certificati non corrispondono, la connessione da FND a SSM viene rifiutata.

Questa condizione può essere rilevata in **server.log**, se la registrazione è impostata per il debug, nel modo seguente:

```
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]:
```

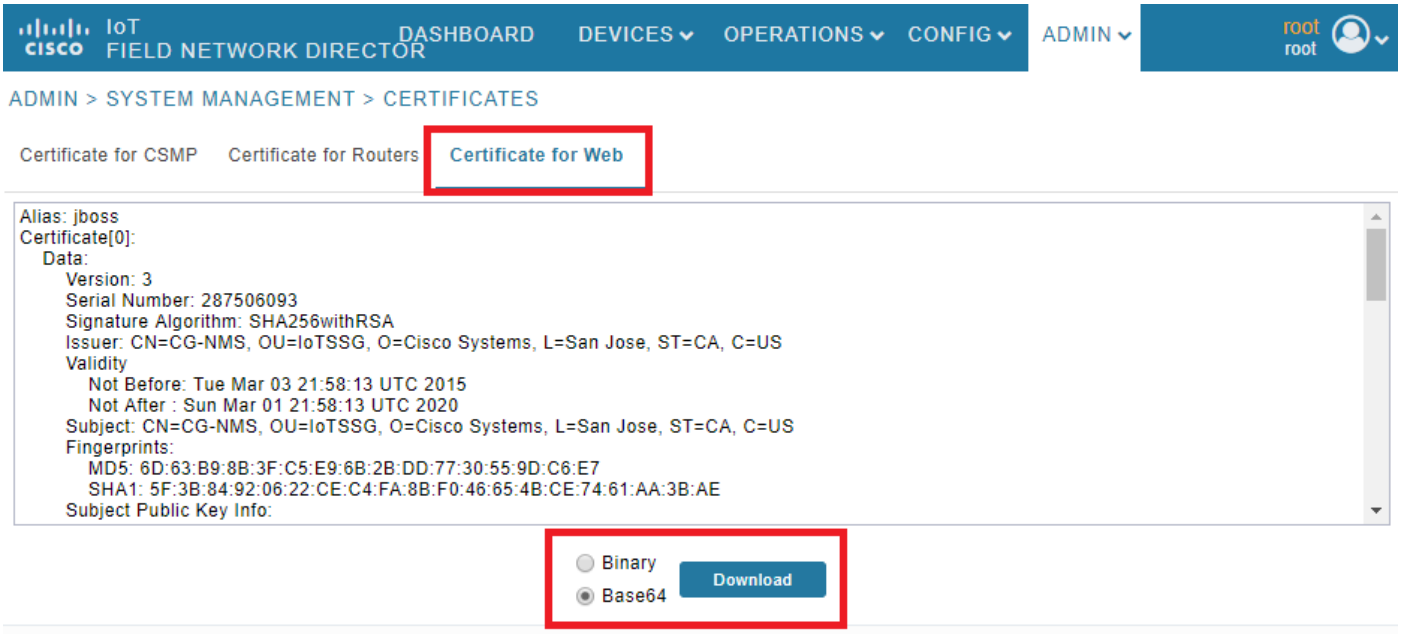
```
javax.net.ssl.SSLPeerUnverifiedException: peer not authenticated
```

Soluzione

Il certificato utilizzato dal server FND per eseguire l'autenticazione client sul server SSM è il certificato Web FND del **jbossas_keystore**.

Affinché SSM consideri attendibile questo certificato, è necessario eseguire i passaggi seguenti:

1. Esportare il certificato Web utilizzando la GUI. Selezionare **Admin > System Management > Certificates > Certificate for Web** (Amministrazione > Gestione sistema > Certificati > Certificato per Web), quindi fare clic su **Download (base64)** come mostrato nell'immagine.



2. Copiare il file di testo o creare un nuovo file sul server FND con il contenuto del certificato del passaggio 1. Per questo esempio, il file viene salvato in **/opt/cgms/server/cgms/conf/webcert.crt**:

```
[root@fndnms ~]# vi /opt/cgms/server/cgms/conf/webcert.crt
[root@fndnms ~]# cat /opt/cgms/server/cgms/conf/webcert.crt
-----BEGIN CERTIFICATE-----
MIIDbTCCAlWgAwIBAgIEESL+rTANBgkqhkiG9w0BAQsFADBnMQswCQYDVQQGEwJV
UzELMAkGA1UECBMCQ0ExETAPBgNVBAcTCFNhbiBKb3NlMRYwFAYDVQQKEw1DaXNj
byBTeXN0ZW1zMQ8wDQYDVQQLEwZJb1RTU0cxDzANBgNVBAMTBkNHLU5NUzAeFw0x
NTAzMDMyMTU4MTNaFw0yMDAzMDEyMTU4MTNaMGcxCzAJBgNVBAYTAlVTMQswCQYD
VQQIEwJDQTERMA8GA1UEBxMIU2FuIEpvc2UxFjAUBgNVBAoTDUNpc2NvIFN5c3Rl
bXMxDzANBgNVBAsTBklvVFNTRzEPMA0GA1UEAxMGQ0ctTk1TMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEAlsgdELNUFi9eXHcb550y0UgbPMgucsKqT1+E
xmwEri517fo+BHdg6AuXpDP4KvLW1/cx8xqWbheKAfPht/HqiFX0ltZdoWaQcaJz
YJOiuL/W3BwQW6UMWPnC1p/Dgnz+qR3JQpR20hC4ymHIIVwKwVfiaJZAnSFNKaZ4
uhOuJDkEC0ZyBbp5Y2Mi9zVRTv/g98p0IqpOjxV0JUtlRkWkjkvCma/Q6dZzSdle
YZzyAS/ud4KVxytKKoxBBDPrtPRbT6lu2VMyWe26cRjPCveZffBABoSvLjptnb7H
mxJMW7EbL+zjTAL/GmHh8J9P16MX7EoePCPCQdwPRdfQ3GkTKwIDAQABoyEwHzAd
BgNVHQ4EFgQUfyFoDj0hJLtUu6ZtKCHuisCQfl4wDQYJKoZIhvcNAQELBQADggEB
AF9fVfEwqbP4BszGHfzTa8pf4zUPJ3Lcz1z6RxwtyGXq8oZK8YQWRpa2NQKLDnve
VjXSdOBvDKRYqPkZeAmTRS0BobeZr2NdHb/FNXMlR6eBm56UrefW+VdQE7syOmGq
Ynlwb/1KF/Fkyp2xVk7nHCtHl+I90l3DlyPmGbQ/TxgA6PXY6V6d571IARNdohYm
qZ/3B+ZK/F4PLOcUwWDtxTBFnlElyq+YjhZiqsCmsxI1GWqleWltUVGMXNM1YLN5
N1KAbOeC0O4n2MqzTWTU9Ss51WfceWsBoSPO+4xyzcRDZmo7IWZiwp4ZAO3eYOz/
```

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

3. Eseguire questo comando per importare il certificato come attendibile in **ssm_web_keystore**:

```
[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. Una volta importato il certificato, riavviare il servizio SSM:

```
[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).
```

Èpossibile verificare se FND è in grado di comunicare con SSM. Selezionare **Amministrazione > Certificati > Certificato per CSMP** nella GUI FND.

Se tutto va bene, dovrebbe essere possibile visualizzare il certificato CSMP in SSM come mostrato nell'immagine.


IoT
FIELD NETWORK DIRECTOR
DASHBOARD
DEVICES
OPERATIONS
CONFIG
ADMIN
root
root
ADMIN > SYSTEM MANAGEMENT > CERTIFICATES
Certificate for CSMP
Certificate for Routers
Certificate for Web
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