

FNDからSSMへの通信のための証明書の設定

内容

[概要](#)

[問題](#)

[解決方法](#)

概要

このドキュメントでは、Field Network Director(FND)とソフトウェアセキュリティモジュール(SSM)間の通信の問題を正しく設定する方法について説明します。

問題

FND 4.4以降、FNDアプリケーションサーバとSSMサービス間の通信には相互認証が必要です。

この相互認証が正しく設定されていないか、証明書が一致しない場合、FNDからSSMへの接続は拒否されます。

ロギングがdebugに設定されている場合は、次のようにserver.logで確認できます。

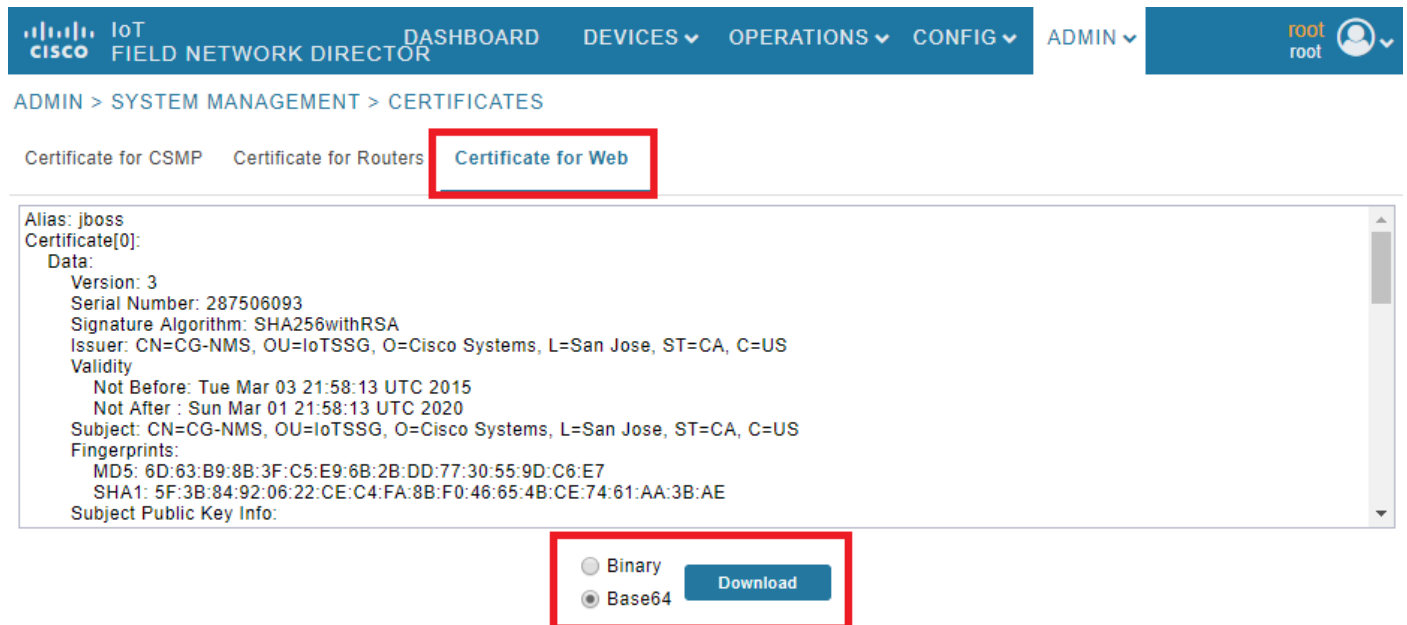
```
7645: SLC-FND: Jun 20 2019 13:22:49.929 +0000: %IOTFND-7-UNSPECIFIED:
%[ch=SSMClient][sev=DEBUG][tid=http-/0.0.0.0:443-5]: Sending request to SSM Server. Request
:https://127.0.0.1:8445/api/v0/ssmws/loadKeyStore.json
7646: SLC-FND: Jun 20 2019 13:22:49.930 +0000: %IOTFND-7-UNSPECIFIED:
%[ch=BasicClientConnectionManager][sev=DEBUG][tid=http-/0.0.0.0:443-5]: 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
```

解決方法

FNDサーバーがSSMサーバー上でクライアント認証を行うために使用する証明書は、jbossa_keystoreからのFND Web証明書です。

SSMがこの証明書を信頼するには、次の手順を実行する必要があります。

1. GUIを使用してWeb証明書をエクスポートします。図に示すように、[Admin] > [System Management] > [Certificates] > [Certificate for Web]に移動し、[Download (base64)]をクリックします。



The screenshot shows the Cisco Field Network Director interface. The top navigation bar includes 'ADMIN' and 'root' user information. The main content area is titled 'ADMIN > SYSTEM MANAGEMENT > CERTIFICATES'. Underneath, there are three tabs: 'Certificate for CSMP', 'Certificate for Routers', and 'Certificate for Web', with the latter being selected and highlighted by a red box. Below the tabs, a scrollable area displays the details of the selected certificate, including its alias 'jbossa', version '3', serial number '287506093', and various cryptographic parameters. At the bottom of this area, there are two radio buttons: 'Binary' and 'Base64', with 'Base64' being selected and highlighted by a red box. To the right of these buttons is a 'Download' button.

2. テキストファイルをコピーするか、ステップ1の証明書の内容を含む新しいファイルをFNDサーバーに作成します。この例では、ファイルは/opt/cgms/server/cgms/conf/webcert.crtに保存されます。

```
[root@fndnms ~]# vi /opt/cgms/server/cgms/conf/webcert.crt
[root@fndnms ~]# cat /opt/cgms/server/cgms/conf/webcert.crt
-----BEGIN CERTIFICATE-----
MIIDbTCCAlWgAwIBAgIEESL+rTANBgkqhkiG9w0BAQsFADBNMQswCQYDVQQGEwJV
UzELMAkGA1UECBMCQ0ExETAPBgNVBACTCFNBhbiBKb3NlMRwYwFAYDVOQKEw1DaXNj
byBTeXN0ZW1zMQ8wDQYDVQQLEwZjb1RTU0cxZDZANBgNVBAMTBkNHLU5NUzAeFw0x
NTAzMDMyMTU4MTNaFw0yMDAzMDUyMTU4MTNaMGcxZzAJBgNVBAYTAlVTMQswCQYD
VQIQIEwJdQTERMA8GA1UEBxMIU2FuIEpvc2UxZjAUBgNVBAoTDUNpc2NvIFN5c3Rl
bXMxZDZANBgNVBAsTBk1vVFNTZzEPMzA0GA1UEAxMGQ0ctTk1TMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEAlsgdELNUFi9eXhcb550y0UgBPmguCsKqTl+E
xmWeri517fo+BHdg6AuXpDP4KvLWl/cx8xqWbheKAfPht/HqiFX0ltZdoWaQcaJz
YJOiuL/W3BwQW6UMWPnClp/Dgnz+qR3JQpR20hC4ymHIIvKwVfiaJZAnSFNkaZ4
uhOuJdKEC0ZyBbp5Y2Mi9zVRTv/g98p0Iqp0jxV0JUtlRkWkjkvCma/Q6dZzSdle
YZzyAS/ud4KVxytKKoxBBDPrTPrBt6lu2VMYwe26cRjPCveZffBABoSVLjptnb7H
mxJMW7EbL+zjTAL/GmHh8J9P16MX7EoePCPCQdwPRdfQ3GkTKwIDAQABoyEwHzAd
BgNVHQ4EFgQUfyFodj0hJLtu6ZtKCHuisCQfl4wDQYJKoZIhvcNAQELBQADggEB
AF9fvfEwqBP4BsZGHfzTa8pf4zUPJ3Lcz1z6RxtwYGXq8oZK8YQWRpa2NQKLDnve
VjXsDoBvDKRYqPkZeAmTRS0BobeZr2NdHb/FNXM1R6eBm56UrefW+VdQE7syOmGq
Ynlwb/1KF/Fkyp2xVk7nHcTh1+I9013DlyPmGbQ/TxgA6PXY6V6d571IARndohYm
qZ/3B+ZK/F4PLOCuWwdtXtBfnlelyq+YjhZiqsCmsxI1GWqlEwltUVGMXNM1YLN5
N1KAbOeC004n2MqzTWTU9Ss51WfceWsBoSPO+4xyzcRDZmo7IWZiwp4ZA03eYOz/
4aUEdBZxv29+QQ7dq6ZZOXQ=
-----END CERTIFICATE-----
```

3. ssm_web_keystoreで信頼できる証明書としてインポートするには、次のコマンドを実行します

o

```
[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.証明書がインポートされたら、SSMサービスを再起動します。

```
[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).
```

FNDがSSMと通信できるかどうかを確認できます。FND GUIで[Admin] > [Certificates] > [Certificate for CSMP]に移動します。

すべてが正常に行われると、図に示すようにSSMでCSMP証明書を確認できます。



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