IoT FND のトラブルシューティング

ここでは、IoT FND の一般的な問題の解決方法について説明します。

- トンネル プロビジョニングの DHCP 設定問題
- メッシュ エンドポイントの登録の問題
- 期限切れデータベース パスワードの回復
- IoT FND データベース パスワードのロック解除
- IoT FND サービスが開始しない
- IoT FND サーバの server.log ファイルに例外がある
- ルート パスワードのリセット
- IoT FND のセカンド サーバがクラスタを形成しない
- サービスが自動的に再起動する IoT FND
- FAR の管理に関する問題
- メッシュ エンドポイントの管理の問題

(注) IoT FND のバージョンについて、常にリリース ノートを参照するようにしてください。

トンネル プロビジョニングの DHCP 設定問題

アドレスの割り当てに問題があると、IoT FND は Tunnel Provisioning Failure イベントをログに記録します。ログ エントリにエラーの詳細が記述されます。

アドレスの割り当てプロセスをモニタするには、次の手順を実行します。

- IoT FND の server.log ファイルをチェックし、IoT FND がトンネルのプロビジョニング時に DHCP 要求を送信しているかを確認します。
- DHCP サーバのログ ファイルをチェックし、IoT FND からの DHCP 要求が DHCP サーバに到達したかを確認します。

要求がサーバに到達していない場合は、次の手順を実行します。

- IoT FND の [Provisioning Settings] ページ([Admin] > [System Management] > [Provisioning Settings])で、DHCP サーバのアドレスが正しいことを確認します。
- IoT FND と DHCP サーバとの間のネットワーク問題を確認します。

DHCP サーバが要求を受信しているにもかかわらず応答していない場合は、次の手順を実行します。

- DHCP サーバのログ ファイルを確認し、DHCP サーバが DHCP 要求に含まれるリンク アドレスからの要求をサポートするよう設定されていることを確認します。リンク アドレスはトンネル プロビジョニング　テンプレートで定義されています。
- DHCP サーバのアドレス プールが満杯でないことを確認します。

DHCP サーバが応答をしていても IoT FND が応答を処理していない場合は、次の手順を実行します。

- リース時間が無限であることを確認します。そうでない場合、IoT FND は応答を処理しません。
- 他のエラーについて、DHCP サーバのログと IoT FND サーバのログを確認します。

メッシュ エンドポイントの登録の問題

ME が IoT FND に登録した理由を確認するために、IoT FND は ME から登録理由コードを収集し、登録問題を診断するのに役立つよう、イベントおよび印刷されたキー値ペアなどの他の関連情報を含むコードをロギングします。

次に、ロギングされたイベントの例を示します。

```
?Event logged: Event(id=0, eventTime=1335304407477, eventSeverity=0, eventSource=cgmesh,
eventMessage=Mesh node registered due to cold  boot: [lastReg: 0, lastRegReason: 1],
NetElement.id=10043, EventType.name=null, lat=1000.0, lng=1000.0, geoHash=null
```

表 1 に、ME 登録の理由コードと関連イベントをリスト表示します。

表 1　メッシュ エンドポイント登録の理由コード

登録の理由コード	コード	イベント タイプの名前	重大度	メッセージ	説明
REASON_UNKNOWN	0	unknownRegReason	INFO	Mesh node registered for unknown reason.	
REASON_COLDSTART	1	coldBoot	INFO	Mesh node registered due to cold boot.	メッセージには、ME の新しい IP アドレスが含まれます。
REASON_ADMIN	2	manualReRegistration	INFO	Mesh node registered due to manual registration.	エンドポイントは、URL フィールドを含まない NMSRedirectRequest を受信しました。
REASON_IP_CHANGE	3	rejoinedWithNewIP	INFO	Mesh node registered with new IP address.	メッセージには、ME の新しい IP アドレが含まれます。
REASON_NMS_CHANGE	4	nmsAddrChange	INFO	Mesh node registered due to NMS address change.	IoT FND の IP アドレスは、NMSRedirect の外部で変更されました（新しい DHCPv6 オプション値が受信されました）。
REASON_NMS_REDIRECT	5	manualNMSAddrChange	INFO	Mesh node registered due to manual NMS address change.	エンドポイントは NMSRedirect 要求を受信しました。
REASON_NMS_ERROR	6	nmsError	INFO	Mesh node registered due to NMS error.	エンドポイントは、IoT FND からエラーを受信しました。

ME の IoT FND への登録時にイベントを生成する以外に、IoT FND は、WPAN 変更の TLV `WPANStatus` を受信した後にもイベントを生成します。

```
Event logged: Event(id=0, eventTime=1335304407974, eventSeverity=0, eventSource=cgmesh,
eventMessage=WPAN change due to migration to better PAN: [lastChanged: 0, astChangedReason: 4],
NetElement.id=10044, EventType.name=null, lat=1000.0, lng=1000.0, geoHash=null)
```

表 2 に、ME の WPAN 変更の理由と対応するイベントを示します。

表 2　メッシュ エンドポイントの WPAN 変更の理由

登録の理由コード	コード	イベント名	重大度タイプ	説明
IEEE154_PAN_LEAVE_UNKNOWN	-1	unknownWPANChange	MAJOR	不明な理由による WPAN 変更。
IEEE154_PAN_LEAVE_INIT	0	meshInit	該当なし	このコードのイベントは生成されません。
IEEE154_PAN_LEAVE_SYNC_TIMEOUT	1	meshConnectivityLost	MAJOR	メッシュ接続の切断による WPAN 変更。
IEEE154_PAN_LEAVE_GTK_TIMEOUT	2	meshLinkKeyTimeout	MAJOR	メッシュ リンク キーのタイムアウトによる WPAN 変更。
IEEE154_PAN_LEAVE_NO_DEF_ROUTE	3	defaultRouteLost	MAJOR	デフォルト ルートの不在による WPAN 変更。
IEEE154_PAN_LEAVE_OPTIMIZE	4	migratedToBetterPAN	MAJOR	より良好な PAN への移行による WPAN 変更。

これらのイベントでは、ME がネットワークから切断されてから再接続するまでの経過時間がメッセージに含められます。IoT FND は、イベントがロギングされてから ME がオフラインだった期間の合計を示します（たとえば 4 hours 23 minutes ago）。

期限切れデータベース パスワードの回復

期限切れパスワードを回復するには、次のコマンドを実行します。

```
su - oracle

sqlplus sys/cgmsDbaAccount@cgms as sysdba
  alter user cgms_dev identified by test;
  alter user cgms_dev identified by password;
  exit;
```

IoT FND データベース パスワードのロック解除

不正な IoT FND データベース パスワードを何回も入力すると、Oracle はユーザ アカウントをロックします。Oracle ソフトウェアを次の例のように使用して、パスワードをロック解除してください。

```
# su - oracle
# sqlplus sys/<database_password>@cgms as sysdba
  alter user cgms_dev account unlock;
  exit;
```

IoT FND サービスが開始しない

IoT FND サービスが開始しない場合は、次の手順を実行します。

1. データベースへの接続を確認します。
   a. IoT FND サーバにルートとしてログインします。
   b. コマンド プロンプトで次のコマンドを入力します。

```
service cgms status
```

c. データベース サーバの IP アドレスと、IoT FND がデータベースに接続できることを確認します。

- IP アドレスが正しくないかまたは IoT FND がデータベースにアクセスできない場合は、**setupCgms.sh** を実行して正しい値を入力します。

d. **service cgms status** コマンドを実行して接続を確認します。

e. IoT FNDを起動します。

2. サーバにインストールされている JRE のバージョンが正しいことを確認します(「System Requirements」を参照)。
3. データベースの移行が正常に実行されたことを確認します。

IoT FND サーバの server.log ファイルに例外がある

server.log ファイルに IoT FND が cgms_keystore ファイルを開けなかったことを示す例外が存在する場合は、IoT FND サーバの cgms.properties ファイルに保存されている cgms_keystore パスワードが正しくありません。

cgms_keystore ファイルのパスワードは、暗号化されて /opt/cgms/server/cgms/conf/cgms.properties ファイルに保存されます。

パスワードを暗号化または復号化するには、/opt/cgms/bin/**encryption_util.sh** スクリプトを使用します。

cgms.properties ファイルでパスワードを確認または更新します。更新が必要な場合は、パスワードを変更した後に IoT FND を再起動します。

ルート パスワードのリセット

IoT FND のルート ユーザ アカウントのパスワードを忘れた場合は、/opt/cgms/bin/**password_admin.sh** スクリプトを実行してパスワードをリセットします。

IoT FND のセカンド サーバがクラスタを形成しない

通常、IoT FND クラスタでのノードの検出は自動的に行われます。複数の IoT FND サーバが同じサブネットに存在すると、クラスタが形成されます。

IoT FND サーバをインストールしたときに、そのサーバがクラスタに参加しない場合は、以下を行ってください。

1. サーバが同じサブネットにあること、相互に ping できること、および同じクラスタ名を共有していることを確認します。
2. /opt/cgms/bin/print_cluster_view.sh スクリプトを実行して、すべてのメンバーのステータスを確認します。
3. クラスタの名前を次のように変更します。
   a. IoT FND のすべてのクラスタ ノードで、HA_PARTITION_NAME パラメータの値を変更してから再起動します。
   b. UDP_MULTICAST_ADDR パラメータの値(一意のマルチキャスト アドレス)を、クラスタ内のすべてのノードに一致するよう変更します。
   c. CLUSTER_BIND_ADDR パラメータの値を、NMS のバインド先とするインターフェイスに変更します。
4. すべてのクラスタ ノードが NTP を使用するよう設定されていることを確認します(「Configuring NTP Service」を参照)。
5. /etc/hosts ファイルを確認し、IP アドレスがローカル サーバのホスト名に正しくマップされていることを確認します。

サービスが自動的に再起動する IoT FND

IoT FND サービスを開始すると、ウォッチドッグ スクリプトが呼び出されます。ウォッチドッグ スクリプトは、IoT FND サービスの状態を確認します。異常を検出すると、ウォッチドッグ スクリプトはその状態を /opt/cgms/server/cgms/log/cgms_watchdog.log ファイルに記録します

ウォッチドッグ スクリプトは、異常な状態が改善したかどうかを判断するために、3 回試行されます。改善しない場合、データベースが到達不能になっていなければ、IoT FND サービスは自動的に再起動します。データベースが到達可能でない場合、ウォッチドッグは IoT FND サービスを停止します。再起動した原因を確認するには、server.log などのログ ファイルを確認します。

IoT FND サーバでルートとして /opt/cgms/bin/deinstall_cgms_watchdog.sh スクリプトを実行することにより、手動でウォッチドッグ プロセスを無効にします。

FAR の管理に関する問題

ここでは、FAR の管理に関する一般的な問題と解決方法について説明します。

証明書の例外

FAR の IoT FND への登録試行時に IoT FND サーバに保存された server.log ファイルに次の例外が表示された場合は、cgms_keystore ファイルに CA サーバ証明書が含まれていないか、または cgms_keystore ファイルにインポートされている CA 証明書が正しくありません。

```
SSLException: Received fatal alert: unknown_ca
```

証明書を cgms_keystore ファイルにインポートする方法については、『Cisco IoT FND Installation Guide, 4.0.x』の「Generating and Installing Certificates」を参照してください。

FAR がリロードし続け、Up の状態に切り替わらない

FAR が IoT FND に接続するたびにリロードし続ける場合、IoT FND が FAR にプッシュした設定が正常に適用されていないためである可能性があります。

設定のプッシュが失敗した原因を確認するには、IoT FND サーバの server.log ファイルをチェックします。[Field Area Router Tunnel Addition] テンプレートへの入力ミスが失敗の原因である場合もあります（IoT FND は、テンプレートを検証しません）。

(注) FAR が IoT FND に登録すると、IoT FND は、show コマンドにより FAR に対してクエリを実行します。IoT FND はその後、[Field Area Router Tunnel Addition] テンプレート内の設定コマンドに基づいて FAR を設定します。

リロードが続く原因には、他に次のものが考えられます。

- パケットをドロップして登録を完了させないようにする、不正な WAN リンク。
- ファイアウォール の問題。ファイアウォールが両方向のトラフィックを許可していること、および、正しいポートを入出力するトラフィックの通過が許可されていることを確認します。

IoT FND で FAR の状態が正しくない

IoT FND で、FAR の ping や FAR へのルートのトレースを問題なく実行できるにもかかわらず、FAR の状態が [Down] と表示される場合があります。

IoT FND は、FAR 上で実行される IoT DM サービスを介して FAR を管理します。そのため、FAR を ping でき、FAR が到達可能な場合も、次により、jetty サーバおよび Call Home 機能が FAR で有効であることを確認する必要があります。

```
'show run callhome' should have 'enable' in the config and 'sh jvm status'
```

メッシュ エンドポイントの管理の問題

ここでは、ME の管理に関する一般的な問題と解決方法について説明します。

メッシュ エンドポイントが IoT FND に登録していない

ME が FAR に接続していること、および IPv6 により IoT FND から ping できることを確認します。ping できる場合は、以下を確認してください。

- クロックが同期されている。
- ME により使用されている DHCP サーバが正しい IoT FND IP アドレスでプログラムされている。
- ME が実行しているイメージが、現在のバージョンの IoT FND と互換性がある。
- HSM が使用されている場合、HSM がオンラインで適切に応答していることが必要です。

ライセンスの問題

ここでは、ライセンスの管理に関する一般的な問題と解決方法について説明します。

デバイス インポートの失敗

IoT FND へのデバイス インポートは、IoT FND サーバ ライセンスの割り当て数に依存します。

IoT FND サーバのライセンス数が、IoT FND データベースにインポートするデバイスの数およびタイプに十分に対応できることを確認します。

IoT FND では、一意のデバイス EID のみが許可されます。IoT FND にこのデバイス EID を インポート済みであったり、現在同じデバイス EID をインポートしようとしているユーザが他にいないことを確認します。他のユーザが同時に同じデバイスを IoT FND にインポートしていないことを確認します。

ライセンス ファイルのアップロードの失敗

期限切れのライセンス ファイルはエラーの原因になります。ライセンス ファイルの有効性および有効期限を確認してください。