OpenLM Server v5へのアップグレード

Version 5 of OpenLM Serverバージョン５はモデルチェンジされており、次は知っておくべき必要な項目です。

コンポーネントの互換性

OpenLM Serverバージョン5のアップグレードは、Serverと連動するコンポーネントのアップグレードをしなければならないという意味でもあります。

バージョン5と互換性のある最小バージョンは次の通りです。

- OpenLM Broker v4.9.0
- OpenLM Agent v5.0.0
- OpenLM Applications Manager v2.3
- OpenLM Reports Scheduler v1.9.8
- OpenLM Router v2.1

アプリケーションポート

デフォルトのOpenLM Serverの通信ポートはこれから5015になります。各アプリケーションごとに設けられていたポートは不要になりました。（Broker、 Agent、 Router等） 全通信は5015で行われます。

バージョン4からアップグレードする場合、設定の変更は必要ですか？

バージョン４からアップグレードする場合、インストーラーは前バージョンのポート設定を検知し、古いポート番号をAPI（7014）、Broker（7016）、Agent（7012）のみ変えないまま保存します。この方法のおかげで、バージョン５に互換性のあるBrokerやAgentが既存のアップグレード予定のOpenLM Server バージョン４を指している状態の場合でも、設定の変更は必要あり

ません。これらの設定は自動的にOpenLM Server/bin/**appsettings.json**ファイルに保存されます。

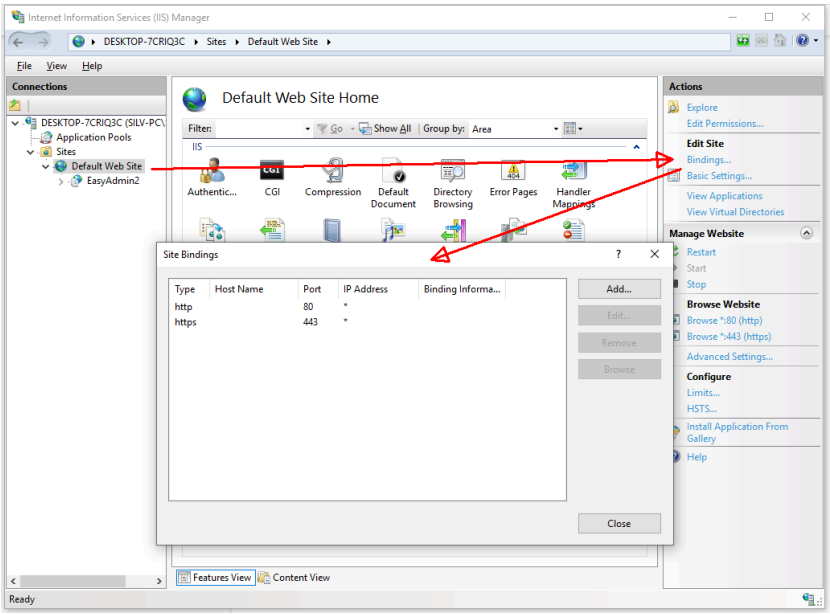
バージョン5を**新規でインストールする**場合は、メインポートは5015になります。Brokerや他のコンポーネントが同じホスト名かIPアドレスを既に指している場合、2つの方法があります。

1. 各コンポーネントの設定を新しいServerポートを指すように変更する。インストールしたコンポーネントが沢山ある場合（例：数百のBroker）、とても大変です。
2. エイリアスのポート設定をOpenLM Server/bin/**a appsettings.json**ファイルに追加する。エイリアスポートは自由なポート番号で大丈夫です。(例： 7016)　そして古いポート番号設定として行動してくれます。
この方法ですと、OpenLM Serverマシンの設定変更のみで完了です。

以前、ServerポートをHTTPS / SSLで設定した場合はどうなりますか？

IISを通して、OpenLMのポートにSSLを以前設定していた場合は、appsettings.jsonファイルで指定されたポートとコンフリクトを起こすIISバインディングを削除しなければいけません。そうしなければServerの処理は開始に失敗してしまいます。SSLを使用するにはマニュアルでの変更が必要です。

1. IISを開く → Sites（サイト） → Default Web Site（デフォルトウェブサイト） → 右パネルで、Bindings（バインディング）をクリックし、EasyAdminに使用されるポート以外でコンフリクトを起こすポートを削除する。



2. **C:\Program Files (x86)\OpenLM\OpenLM Server\WebApps\EasyAdmin2\params.js**ファイルをアドミン権限にてテキストエディターで開く。プロトコールをHTTP**S**に編集する。DNS名がSSL証明書と完全一致するようにする。 (例：ホスト名.com等)

```
var _operationMode = "";
var _enableDemoMode = false;
var _debug = false;
var _useProxy = true;
var _sampleMode = false;
var _schedulingTaskURL = 'http://127.0.0.1:8888/report_scheduler/job';
var _SAASLoginURL = 'https://saas.openlm.com/SaasClient/Home/Login';
var SoapProxyPath = 'https://SILV-PC:5015/OpenLM.Server.Services/AdminAPI/web';
var WebProxyPath = 'https://SILV-PC:5015/OpenLM.Server.Services/AdminAPI/web';
var WebProxySaasPath = 'https://SILV-PC:8084/SaasService/service.svc';
var OpenLMServer = 'https://SILV-PC:5015/api/easyadminapi/postmessage';
var EasyadminRoot  = 'https://SILV-PC/easyadmin_trunk/';
var _angularURL = "";
var Locales = [["en_US", "English US", "UTF-8"],
    ["es_ES", "Español - España", "ISO-8859-1"],
    ["de_DE", "Deutsch - Deutschland", "ISO-8859-1"],
    ["fr_FR", "Française - France", "ISO-8859-1"],
    ["nl_NL", "Dutch - Nederland", "ISO-8859-1"],
    ["pt_BR", "Português - Brazil", "ISO-8859-1"],
    ["ja_JP", "日本語 - 日本", "UTF-8"],
    ["zh_CN", "汉语 - 中国", "UTF-8"]];
```

3. アドミン権限にて**C:\Program Files (x86)\OpenLM\OpenLM Server\bin\appsettings.json**ファイルをテキストエディターで開く。

4. ファイルの末尾で、次のように編集する。

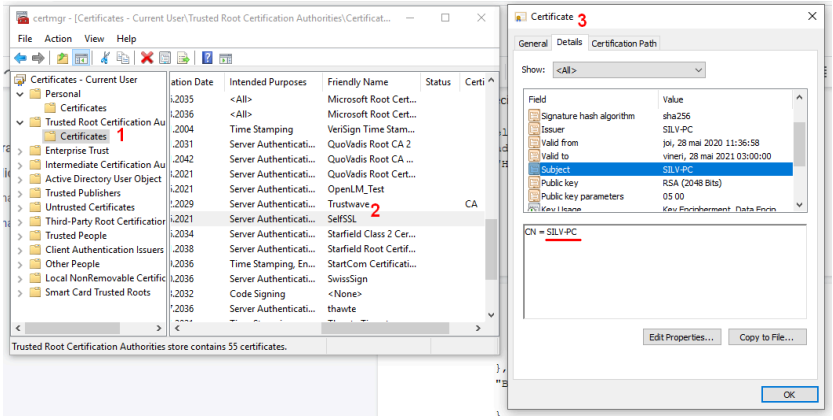
- “Url”変数をHTTP**S**を指すように編集
- 証明書ストアか証明書への特定パスをしようするかで“Kestrel”ノードを編集する
- 必要なら、メインにエイリアスとして行動するポートを追加できます。””で挟まれた名前(例： “Broker”)は記述方式で値を保持できます。

a) Windowsストアから証明書を使用する場合

```
"Kestrel": {
    "Endpoints": {
      "Http": {
        "Url": "https://*:5015"
      },
      "Broker": {
        "Url": "https://*:7016"
      },
      "Agent": {
        "Url": "https://*:7012"
      }
    },
    "Certificates": {
      "Default": {
        "Subject": "SILV-PC",
        "Store": "Root",
        "Location": "LocalMachine",
        "AllowInvalid": "true"
      }
    }
```

```
}
```

“Subject”（主題）は証明書のオーナーの場所、誰に発行されたか。Run（実行） → certmgr.msc → select the certificate store where your certificate resides（証明書が存在する証明書ストアを選択する） → ダブルクリック → 詳細タブをクリック→ Subjectを検索



“Store”（ストア）は証明書ストアを示します。“Personal”（個人）ストアは”My”として参照され、“Trusted Root Certification Authorities”（信頼されたルート証明書機関）は”Root”として参照されます。他の証明書ストアの名前として、この文書を参考にしてください。

“Location”（場所）はLocalMachineかCurrentUserのいずれかです。

“AllowInvalid” をtrue に設定して無効な証明書の使用を許可するようにしてください。（例： self-signed certificates 自己サイン証明書)

b) 特別なパスを持つ証明書の使用の場合

```
"Kestrel": {

    "Endpoints": {

      "Http": {

        "Url": "https://*:5015"
```

```
    },
    "Broker": {
      "Url": "https://*:7016"
    },
    "Agent": {
      "Url": "https://*:7012"
    }
  },
  "Certificates": {
    "Default": {
      "Path": "C:\\Users\\borisi\\Desktop\\Cer
      "Password": "ZXzx12!@"
    }
  }
}
```

- **Path（パス）**は証明書ファイルへのパスです。Windowsのパスではスラッシュではなくバックスラッシュを2つ使用するようにしてください（日本語環境では￥マーク）。
- **Password**は証明書のプライベートキーのパスワードです。
- } で {　に合わせてきちんと閉じられているか確認してください。

5. ファイルを保存。

6. “OpenLM Server”サービスを再開。

> **重要**: オプションa)とb) ではOpenLM Serverに接続するマシンに証明書がインストールされており、その証明書ストアに存在することも必須で前提です。（例： Agent）

ライセンスファイル

バージョン4のライセンスファイルはOpenLM Serverバージョン5と互換性はありません。新しいライセンスファイルを営業**sales@openlm.com**にお問い合わせください。

LDAP同期

LDAP同期はバージョン５から分離され、Directory Synchronizationと呼ばれる別のコンポーネントで提供されるようになりました。LDAP機能（ユーザーをドメインディレクトリと同期）を継続して使用したい場合、Directory Synchronization Service (DSS)とDirectory Synchronization Agent (DSA)をインストールする必要があります。

DSSとDSAなしでアップグレードしたら現行の同期データを失いますか？

答えはNoです。
DSSとDSAのインストールなしでアップグレードした場合、既存の同期定義や関連する全データは保存されたままです。しかし非アクティブになります。DSSとDSAをインストールすれば、既存の同期定義をDSSに移行でき、LDAP同期機能を以前の様に継続して使用することができます。