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 \rightarrow Sites(サイト) \rightarrow Default Web Site(デフォルト ウェブサイト) \rightarrow 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。

<u>File View H</u> elp		
Connections	Default Web Site Home	Actions
STATESKTOP-7CRIO3C (SILV-PC)	•	Explore
Application Pools	Filter: • 🐨 💁 • 🥁 Show All Group by: Area • 🔛 •	Edit Site
V 🙆 Sites		Bindings
> BasyAdmin2		Basic Settings
	Authentic CGI Compression Default Directory Error Pages Handler	View Applications
		View Virtual Director
		Manage Website
Sit	Bindings ?	× Restart
	Ener Hand Name Dark ID Address Diadian Information Add	Stop
	type Plost Name Port iP Address binding informa Add	Browse Website
	ttps 443 *	Browse *:80 (http)
	Remov	e Browse *:443 (https)
	Proversi	Advanced Settings.
	0.0112	Configure
		HSTS
		Install Application F
		Help
		_
	Close	

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HTTPS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)

1	<pre>var _operationMode = "";</pre>
2	<pre>var _enableDemoMode = false;</pre>
3	var _debug = false;
4	<pre>var _useProxy = true;</pre>
5	<pre>var _sampleMode = false;</pre>
6	<pre>var _schedulingTaskURL = 'http://127.0.0.1:8888/report_scheduler/job';</pre>
7	<pre>var _SAASLoginURL = 'https://saas.openlm.com/SaasClient/Home/Login';</pre>
8	<pre>var SoapProxyPath = 'https://SILV-PC:5015/OpenLM.Server.Services/AdminAPI/web';</pre>
9	<pre>var WebProxyPath = 'https://SILV-PC:5015/OpenLM.Server.Services/AdminAPI/web';</pre>
10	<pre>var WebProxySaasPath = 'https://SILV-PC:8084/SaasService/service.svc';</pre>
11	<pre>var OpenLMServer = 'https://SILV-PC:5015/api/easyadminapi/postmessage';</pre>
12	<pre>var EasyadminRoot = 'https://SILV-PC/easyadmin_trunk/';</pre>
13	var _angularURL = "";
14	<pre>var Locales = [["en_US", "English US", "UTF-8"],</pre>
15	["es_ES", "Español - España", "ISO-8859-1"],
16	["de_DE", "Deutsch - Deutschland", "ISO-8859-1"],
17	["fr_FR", "Française - France", "ISO-8859-1"],
18	["nl_NL", "Dutch - Nederland", "ISO-8859-1"],
19	["pt_BR", "Português - Brazil", "ISO-8859-1"],
20	["ja_JP", "日本語 - 日本", "UTF-8"],
21	["zh_CN", "汉语 - 中国", "UTF-8"]];
22	

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HTTPS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) \rightarrow certmgr.msc \rightarrow 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) \rightarrow ダブルクリック \rightarrow 詳細タブをクリック \rightarrow Subjectを検索

I	🚰 certmgr - [Certificates - Current U	Jser\Trusted F	Root Certification Autho	rities\Certificat —		×	Certificate 3		×
-	File Action View Help					General Details Certification Path			
ra lic na	Certificates - Current User Certificates Current User Certificate Current Of Certification Au Certificate Certifica	ation Date i.2035 i.2036 .2004 .2031 .2042 .2021 .2021 .2021 .2029 i.2021 .2034 .2038 I.2036 .2038 .2036 .2032 .2036 .2032 .2036 .2036 .2035 .2036 .2037 .2038 .2036 .2038 .2036 .2038 .2038 .2038 .2038 .2038 .2038 .2038 .2038 .2038 .2039 .2031 .2039 .2031 .2042 .2021 .2021 .2021 .2021 .2021 .2021 .2031 .2034 .2034 .2031 .2021 .2034 .2034 .2034 .2034 .2034 .2034 .2034 .2034 .2034 .2034 .2034 .2034 .2034 .2034 .2034 .2034 .2034 .2034 .2035 .2034 .2034 .2038 .2036 .2038 .2036 .2036 .2038 .2036	Intended Purposes <all> <all> Server Authenticati Server Authenticati Server Authenticati Server Authenticati Server Authenticati Server Authenticati Server Authenticati Server Authenticati Code Signing Server Authenticati Strever Authenticati Strever Authenticati Strever Authenticati Strever Authenticati Strever Authenticati Strever Authenticati Strever Authenticati Strever Authenticati Strever Authenticati</all></all>	Friendly Name Microsoft Root Cett. Versign Time Stam. Versign Time Stam. Versign Root Cett. QuoVadis Root C.A. QuoVadis Root C.A. QuoVadis Root C.A. QuoVadis Root C.A. Starfield Root Cettif Starfield Root Cettif Starfield Root Cettif Starfield Root Cettif Starfield Root Cettif	Status	Certi ^ rci ;1 ;d ;H CA ; ; ; ; ; ; ;	Show: Al> Field Sognature hash algorithm Sognature hash algorithm Sognature hash algorithm Valid fon Valid fon Pablic key parameters Micro Lapor	Value sha256 SILV+PC Jo, 28 ma 2020 11:36:58 viver, 28 ma 2020 12:30:00 OS 00 Key Encidement Data Ench Edit Properties Copy to File	•

"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。

OpenLM Server v5へのアップグレード - OpenLM Japan

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@openIm.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。

+81 (0)50 5893 6263

sales@openIm.com