OpenAM 14 インストールガイド

OSSTech(株)

更新日 2024 年 8 月 9 日
リビジョン 1.15

目次

1 はじめに

1.1 本書の目的

本文書は、弊社提供の OpenAM 14 パッケージのインストールを実施するための手順書です。 OpenAM 14 パッケージのインストールやアップデートの際には、必ず本文書の内容を確認してから作業を実施してください。

本文書に関する記載内容について疑問点等がある場合には、弊社サポート窓口までお問い合わせください。

1.2 前提条件

本書は、特に指示がない限り、以下のような条件を前提に記述しています。これと異なる場合は、適宜内容を読み替えるか、必要な作業を別途実施してください。

- 作業者が OS と関連ソフトウェアの管理や操作手順についての一般的な知識を有すること。
- OS と関連ソフトウェアの基本設定が適切になされていること。
- 管理ユーザー root のシェル端末で作業すること。(作業ユーザーを指定している場合を除く)
- 製品パッケージファイル群をインストール対象環境の `/srv/osstech-work/software/RPMS` ディレクトリ以下にコピーしておくこと。

1.3 略語

本文書では必要に応じて以下のような略語を用います。

- 「Red Hat Enterprise Linux」を「RHEL」と表記します。

2 事前準備

本章では、OpenAM のインストールを開始する前の確認事項について説明します。

2.1 ホスト名の名前解決

OpenAM はシングルサインオンを実現するためにドメインクッキーを発行します。そのため OpenAM サーバーに対しては、完全修飾ドメイン名 (FQDN) でアクセスする必要があります。FQDN が DNS 等により名前解決可能であることを確認して下さい。

なお、本書では OpenAM サーバーのホスト名を「openam01.example.co.jp」として説明します。

3 システム要件

3.1 ソフトウェア要件

以下のいずれかの OS 環境が必要です。

- Red Hat Enterprise Linux 9 / AlmaLinux 9 / Rocky Linux 9 (x86-64)
  - 本書ではこれらの OS を RHEL9 系 と表記します
- Red Hat Enterprise Linux 8 / AlmaLinux 8 / Rocky Linux 8 (x86-64)
  - 本書ではこれらの OS を RHEL8 系 と表記します
- Red Hat Enterprise Linux 7 / CentOS 7 (x86-64)
  - 本書ではこれらの OS を RHEL7 系 と表記します

また、以下のソフトウェアが必要です。

- OS 標準 OpenJDK 11 (RHEL7 系)
- OS 標準 OpenJDK 21 (RHEL9 系及び RHEL8 系)

以下のソフトウェアの使用を推奨します。

- Apache HTTP Server

Apache HTTP Server は必須ではありませんが、HTTP リクエストを Apache で受けて AJP で Tomcat と通信する構成を推奨します。

3.2 対応ブラウザー

対応するブラウザーについては製品ページの動作確認済みブラウザーの欄をご確認下さい。

なお、初期設定及びアップグレードには Internet Explorer 11 は利用できません（シングルサインオンでの利用は可能です）。

4 パッケージ構成

弊社が提供する Linux 版ソフトウェアは以下のパッケージにより構成されています。

1. OSSTech ソフトウェア製品基本パッケージ

- osstech-base
- osstech-support

2. OSSTech Tomcat パッケージ

- osstech-tomcat (RHEL9 系及び RHEL8 系)
- osstech-tomcat9 (RHEL7 系)

3. OSSTech OpenAM 14 パッケージ

- osstech-openam14

5 RPM パッケージのインストール

各パッケージのインストールは、OS 付属の rpm コマンドを用いて行います。以下の手順にしたがってパッケージのインストールを実施してください。

5.1 準備

パッケージのインストールは、root ユーザーのみに許可されていますので、su コマンドで root ユーザーになります。

```
$ su -
Password: root のパスワードを入力（ 画面には表示されません ）
```

次に弊社から提供されたパッケージ一式をインストール先ホストの任意のディレクトリに展開します。

以降は `/srv/osstech-work/software/RPMS` に展開したことを前提として記述します。

5.2 パッケージの確認

パッケージ展開先のディレクトリに弊社提供のパッケージ一式があることを確認します。

- RHEL9 系及び RHEL8 系の場合

```
# cd /srv/osstech-work/software/RPMS
# ls
install.sh  noarch
# ls noarch
osstech-base-x.x-x.el9.noarch.rpm
osstech-openam14-14.x.x-x.el9.noarch.rpm
osstech-openam14-configtools-14.x.x-x.el9.noarch.rpm
osstech-openam14-tools-14.x.x-x.el9.noarch.rpm
osstech-support-x.x-x.el9.noarch.rpm
osstech-tomcat-9.x.x-x.el9.noarch.rpm
repodata
```

RHEL8 系の場合、ファイル名の el9 は el8 となります。

- RHEL7 系の場合

```
# cd /srv/osstech-work/software/RPMS
# ls
install.sh  x86_64
# ls x86_64
osstech-base-x.x-x.el7.x86_64.rpm
osstech-openam14-14.x.x-x.el7.noarch.rpm
osstech-openam14-configtools-14.x.x-x.el7.noarch.rpm
osstech-openam14-tools-14.x.x-x.el7.noarch.rpm
osstech-support-x.x-x.el7.x86_64.rpm
osstech-tomcat9-9.x.x-x.el7.noarch.rpm
repodata
```

5.3 パッケージのインストール

yum でパッケージインストールができる環境の場合、以下のコマンドを実行しインストールを実施します。

```
# ./install.sh
```

コマンドを実行すると「Is this ok [y/N]:」という出力があります。ここで「y」を入力すると、依存パッケージも含めてパッケージ一式がインストールされます。

この「install」コマンドは「yum」に依存しています。したがって、これまで yum コマンドを実行したことがない場合はもう一度「Is this ok [y/N]:」という出力があります。問いかけの意味については yum のマニュアルをご覧ください。

以下の出力が得られれば完了です。

```
完了しました!（もしくは Complete!）
```

yum でパッケージインストールができない環境の場合、依存パッケージインストール後、以下のように rpm コマンドを使用してパッケージインストールを実施します。

- RHEL9 系及び RHEL8 系の場合

```
# cd noarch
# rpm -ivh osstech-base*.rpm \
> osstech-support*.rpm \
> osstech-tomcat*.rpm \
> osstech-openam14-14.*.rpm \
```

```
> osstech-openam14-tools-*.rpm
```

- RHEL7 系の場合

```
# cd x86_64
# rpm -ivh osstech-base*.rpm \
> osstech-support*.rpm \
> osstech-tomcat*.rpm \
> osstech-openam14-14.*.rpm \
> osstech-openam14-tools-*.rpm
```

どちらの場合も以下の出力が得られれば完了です。

```
...(省略) [100%]
```

5.4 Apache を構成

HTTP リクエストを Apache で受けて AJP で Tomcat と通信する構成を構築します。Apache を使用せず Tomcat の HTTP コネクタを使用する場合は、本節を実施する必要はありません。

5.4.1 Apache のインストール

yum コマンドで Apache HTTP Server をインストールします。

```
# yum install -y httpd mod_ssl
```

5.4.2 Apache の設定

8080 ポートで Listen し、Tomcat と AJP 通信を行うよう Apache の設定に追加します。

```
Listen 8080
ProxyPass /openam ajp://localhost:8009/openam retry=0
```

Apache と Tomcat が同一サーバーであるため retry=0 を付けています。

5.4.3 SELinux の設定

本項は **SELinux が有効な環境のみ**実施します。 Apache がリバースプロキシサーバーとして動作できるように SELinux の設定を行います。

```
# setsebool -P httpd_can_network_relay on
```

5.4.4 Apache の起動

Apache を起動します。

```
# systemctl start httpd
```

5.5 Tomcat HTTP コネクターの設定変更

本節は **Apache を利用しない場合のみ**設定します。 Tomcat で 8080 ポートを利用できるように `/opt/osstech/etc/tomcat` ディレクトリにある server.xml を変更します。

```
<Connector protocol="HTTP/1.1"
           address="[ポートをリッスンする IP アドレス]"
           port="8080"
           connectionTimeout="20000"
           redirectPort="8443" />
```

5.6 Tomcat の起動

RPM パッケージをインストール後、Tomcat を起動します。

```
# systemctl start osstech-tomcat
```

5.7 初期設定の開始

Tomcat が起動したら、ブラウザーで以下の URL にアクセスします。

- http://openam01.example.co.jp:8080/openam/

「設定オプション画面」が表示されます。この画面から OpenAM の初期設定を行います。コンテキスト名 (/openam/) は変更可能です。コンテキスト名を変更する場合は Tomcat を起動する前に「コンテキスト名の変更」を実施ください。

SELinux が有効な環境では、OpenAM 初期設定後に SELinux に関する設定を実施する必要があります。具体的な手順は OpenAM 14 初期設定ガイド （冗長構成） のドキュメントを参照してください。

図 1　設定オプション画面

6 RPM パッケージのアップデート

弊社提供のパッケージをアップデートする際は、以下の手順にしたがって実施してください。2 台構成の場合は「OpenAM 2 台構成のアップデート」をご覧ください。

6.1 準備

パッケージのインストールは、root ユーザーのみに許可されていますので、su コマンドで root ユーザーになります。

```
$ su -
Password: root のパスワードを入力 ( 画面には表示されません )
```

次に弊社から提供されたパッケージ一式をインストール先ホストの任意のディレクトリに展開します。

以降は `/srv/osstech-work/software/RPMS` に展開したことを前提として記述します。

6.2 OpenJDK 21 のインストール (RHEL9 系及び RHEL8 系)

OpenAM 14.5.0-39 から RHEL9 系及び RHEL8 系環境の OpenAM は OpenJDK 21 で動作するよう変更されました。 OpenJDK 21 がインストールされていない場合はインストールしてください。

```
# yum install java-21-openjdk-headless
```

6.3 Tomcat の停止

Tomcat を停止します。

```
# systemctl stop osstech-tomcat
```

6.4 OpenAM 設定ディレクトリのバックアップ

現在の OpenAM の設定をバックアップします。

下の例では OpenAM の設定の保存先は「/opt/osstech/var/lib/tomcat/data/openam」、バックアップ先は「/root/backup/conf」です。

```
# mkdir -p /root/backup/conf
# cd /opt/osstech/var/lib/tomcat/data
# cp -pir openam /root/backup/conf
```

6.5 Tomcat の work ディレクトリの削除

Tomcat の work ディレクトリを削除します。

```
# rm -rf /opt/osstech/var/cache/tomcat/work/Catalina/localhost/openam
```

6.6 パッケージの確認

パッケージ展開先のディレクトリに弊社提供のパッケージ一式があることを確認します。

- RHEL9 系及び RHEL8 系の場合

```
# cd /srv/osstech-work/software/RPMS
# ls
install.sh  noarch
# ls noarch
osstech-base-x.x-x.el9.noarch.rpm
osstech-openam14-14.x.x-x.el9.noarch.rpm
osstech-openam14-configtools-14.x.x-x.el9.noarch.rpm
osstech-openam14-tools-14.x.x-x.el9.noarch.rpm
osstech-support-x.x-x.el9.noarch.rpm
osstech-tomcat-9.x.x-x.el9.noarch.rpm
repodata
```

RHEL8 系の場合、ファイル名の el9 は el8 となります。

- RHEL7 系の場合

```
# cd /srv/osstech-work/software/RPMS
# ls
install.sh  x86_64
# ls x86_64
osstech-base-x.x-x.el7.x86_64.rpm
osstech-openam14-14.x.x-x.el7.noarch.rpm
osstech-openam14-configtools-14.x.x-x.el7.noarch.rpm
```

```
osstech-openam14-tools-14.x.x-x.el7.noarch.rpm
osstech-support-x.x-x.el7.x86_64.rpm
osstech-tomcat9-9.x.x-x.el7.noarch.rpm
repodata
```

6.7 パッケージのアップデート

パッケージのアップデートを rpm コマンドで行います。

- RHEL9 系及び RHEL8 系の場合

```
# cd noarch
# rpm -Uvh osstech-base*.rpm \
> osstech-support*.rpm \
> osstech-tomcat*.rpm \
> osstech-openam14-14.*.rpm \
> osstech-openam14-tools-*.rpm
```

- RHEL7 系の場合

```
# cd x86_64
# rpm -Uvh osstech-base*.rpm \
> osstech-support*.rpm \
> osstech-tomcat*.rpm \
> osstech-openam14-14.*.rpm \
> osstech-openam14-tools-*.rpm
```

既に最新のパッケージがインストール済みの場合、次のエラーが表示されます。この場合はインストール済みのパッケージをアップデートする必要はありませんので、アップデート不要なパッケージを rpm コマンドの引数から取り除き、再度アップデートを試みます。

```
準備しています...                ################################# [100%]
      パッケージ osstech-base-3.1-149.elx.noarch は既にインストールされています。
      パッケージ osstech-support-3.1-149.elx.noarch は既にインストールされています。
```

上記の例の場合、osstech-base パッケージと osstech-support パッケージのアップデートが不要なことを表しています。

以下のように osstech-xui-login.png.rpmsave ファイルが作成される警告が表示された場合は、OpenAM 14.1 より前のバージョンからアップデートを参照ください。

```
Cleaning up / removing...
   2:osstech-openam14-14.0.0-xx.elx   warning: /opt/osstech/share/tomcat/webap
ps/openam/XUI/images/osstech-xui-login.png saved as /opt/osstech/share/tomcat/
webapps/openam/XUI/images/osstech-xui-login.png.rpmsave
```

web.xml.rpmnew ファイルが作成される警告が表示された場合は、OpenAM 14.2 より前のバージョンからアップデートを参照ください。

```
Updating / installing...
   1:osstech-openam14-14.2.0-0.elx    warning: /opt/osstech/share/tomcat/webap
ps/openam/WEB-INF/web.xml created as /opt/osstech/share/tomcat/webapps/openam/
WEB-INF/web.xml.rpmnew
```

openam.conf.rpmnew ファイルが作成される警告が表示された場合は、OpenAM 14.5.0-39 以降へのアップデートを参照ください。

```
Updating / installing...
   1:osstech-openam14-14.5.0-xx.elx    warning: /opt/osstech/etc/tomcat/tomcat
.conf.d/openam.conf created as /opt/osstech/etc/tomcat/tomcat.conf.d/openam.co
nf.rpmnew
```

6.8 Tomcat の起動

```
# systemctl start osstech-tomcat
```

6.9 アップグレードの実行

1. Tomcat が起動したら、ブラウザーで OpenAM 管理者でログインする際の URL にアクセスします。

- 本書の構成の場合は以下の URL です。
  - http://openam01.example.co.jp:8080/openam/

2. 「アップグレード画面」の「OPENAM 14.x.x へのアップグレード」のボタンをクリックします。

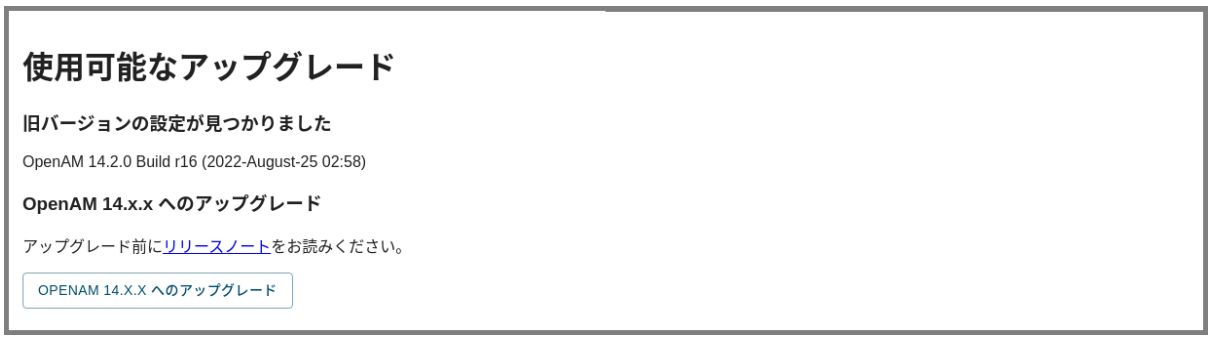

図 2　アップグレード画面

3. 「ライセンス同意画面」をスクロールし、「I accept the license agreement」にチェックして「CONTINUE」ボタンをクリックします。

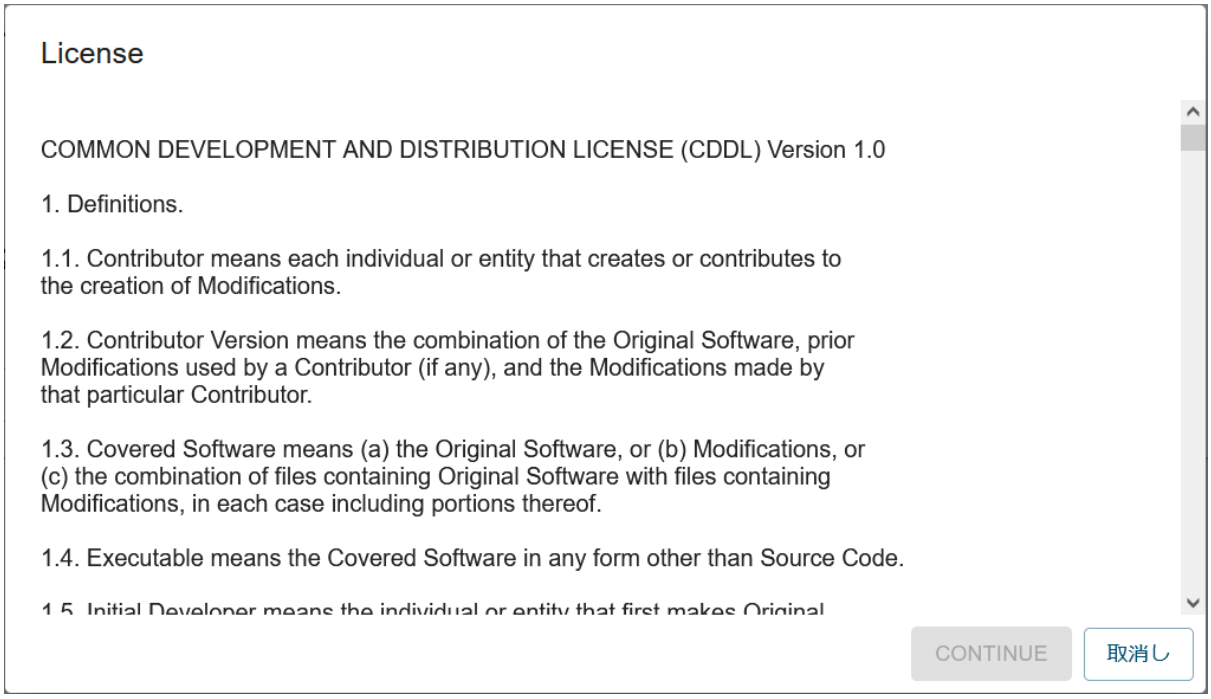

図 3　ライセンス同意画面

4. 確認画面で「アップグレード」ボタンをクリックして OpenAM をアップグレードします。

図 4　アップグレード確認画面

5. OpenAM のアップグレードが完了すると以下の画面が表示されます。

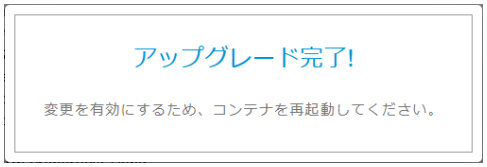

図 5　アップグレード完了画面

6.10 Tomcat 再起動

Tomcat を再起動します。

```
# systemctl restart osstech-tomcat
```

以上で、アップデート作業は完了です。

6.11 OpenAM 2 台構成のアップデート

本節では OpenAM が 2 台で構成される場合のアップデート手順について説明します。サービスを停止せずにアップデートする手順については「ローリングアップデート」を参照してください。

1. OpenAM 1 号機・2 号機それぞれの号機で「準備」と「Tomcat の停止」、「OpenAM 設定ディレクトリのバックアップ」を行います。
2. OpenAM 1 号機・2 号機で「Tomcat の work ディレクトリの削除」と「パッケージの確認」、「パッケージのアップデート」、「Tomcat の起動」を行います。
3. OpenAM 1 号機で「アップグレードの実行」を行います。
   - 1 号機のサーバーホスト名 (FQDN) でアクセスします。
   - OpenAM 2 号機での作業は不要です。
4. OpenAM 1 号機・2 号機で「Tomcat 再起動」を行います。

以上で 2 台構成のアップデート作業は完了です。

6.11.1 ローリングアップデート

本項では OpenAM が 2 台で構成される場合にサービスを停止せずにアップデートする手順 (ローリングアップデート) について説明します。

SAML のポリシー保護機能を利用している場合はこの手順でアップデートを実施することができません。詳細は OpenAM 14.5 より前のバージョンからアップデートをご確認ください。

1. 「準備」と「Tomcat の停止」と「OpenAM 設定ディレクトリのバックアップ」を行います。
   - OpenAM 1 号機・2 号機でそれぞれの号機で実行し、バックアップを取得します。
   - 本作業は片系ずつ実施可能です。片系ずつ実施する場合はもう一方を起動させた状態で取得します。
2. 2 号機のみ Tomcat を起動しておきます。
   - 負荷分散装置の振り分け設定を行い、利用者のアクセスを OpenAM 2 号機のみへ振り分けます。
   - OpenAM 1 号機にはアクセスが届かないようにします。
3. OpenAM 1 号機で「Tomcat の work ディレクトリの削除」と「パッケージの確認」と「パッケージのアップデート」を行います。
4. 続けて OpenAM 1 号機で「Tomcat の起動」と「アップグレードの実行」と「Tomcat 再起動」を行います。
   - 「アップグレードの実行」では 1 号機のサーバーホスト名 (FQDN) でアクセスします。
5. 負荷分散装置の設定を変更し、利用者のアクセスを OpenAM 1 号機のみに振り分け

ます。 OpenAM 2 号機の「Tomcat の停止」を行い、Tomcat を停止します。

6. OpenAM 2 号機で「Tomcat の work ディレクトリの削除」と「パッケージの確認」と「パッケージのアップデート」を行います。
7. OpenAM 2 号機で「Tomcat の起動」を行い、Tomcat を起動します。
    - OpenAM 2 号機では「アップグレードの実行」の作業は不要です。
8. 負荷分散装置の設定を元の状態 (OpenAM 1、2 号機の 2 台に振り分けられる状態) に戻します。

以上でローリングアップデートは完了です。

7 WAR ファイルのデプロイ

OpenAM の WAR ファイルをアプリケーションサーバーにデプロイすることも可能です。本章では Tomcat にデプロイする手順を説明します。

Tomcat は事前にインストールされているものとします。(Tomcat がインストールされているディレクトリを `{TOMCATDIR}` と記載します)

7.1 OpenJDK のインストール

OpenAM の動作には、RHEL9 系及び RHEL8 系環境の場合は OpenJDK 21、RHEL7 系環境の場合は OpenJDK 11 が必要です。OpenJDK がインストールされていない場合はインストールしてください。

- RHEL9 系及び RHEL8 系の場合

```
# yum install java-21-openjdk-headless
```

- RHEL7 系の場合

```
# yum install java-11-openjdk-headless
```

7.2 環境変数 JAVA_HOME の設定

OpenJDK がインストールされ、環境変数「JAVA_HOME」が正しく設定されていることを確認して下さい。

RHEL9 系及び RHEL8 系環境の場合は OpenJDK 21、RHEL7 系環境の場合は OpenJDK 11 のディレクトリが指定されている必要があります。

7.3 環境変数 CATALINA_OPTS の設定 (RHEL9 系及び RHEL8 系)

RHEL9 系及び RHEL8 系環境の場合、OpenAM を OpenJDK 21 で動作させるために JVM オプションを指定する必要があります。Tomcat を使用する場合、JVM オプションは環境変数「CATALINA_OPTS」により指定します。

指定する必要がある JVM オプション及び JVM オプションの指定方法については「Ope-

nAM 14.5.0-39 以降へのアップデート」を参照ください。

7.4 Java ヒープサイズの設定

OpenAM を動作させる環境では、Java のヒープサイズを 2048MB 以上に設定することを推奨します。ヒープサイズは環境変数 JAVA_OPTS により指定できます。

以下はコマンドラインで指定する例です。

```
$ export JAVA_OPTS="-Xmx2048m -XX:MetaspaceSize=256m"
```

その他、OS 起動時に実行されるスクリプト内や、Tomcat の起動スクリプト内などで JAVA_OPTS を指定することもできます。なお、OSSTech Tomcat パッケージでは、サーバーのメモリに応じて値が決定 (最小 2048MB) されるようになっており、この設定は不要です。

7.5 OpenAM WAR ファイルの取得

OpenAM の WAR ファイルは OSSTech 版 OpenAM 14 パッケージの RPM(osstech-openam14) に含まれており、以下のパスにインストールされます。

- /opt/osstech/share/openam14/openam.war

WAR ファイルは以下の 2 通りの方法で取得可能です。

1. 「RPM パッケージのインストール」の手順で RPM をインストールし、上記のパスにインストールされた WAR ファイルを利用する。
2. RPM ファイルをインストールせずに展開し、WAR ファイルを取得する。

ここでは、後者の方法を説明します。

まず、rpm2cpio コマンドと cpio コマンドを利用して RPM ファイルを展開します。

```
$ rpm2cpio osstech-openam14-14.x.x-x.elx.noarch.rpm | cpio -id
```

上記コマンドを実行すると、RPM に含まれるファイルがカレントディレクトリに展開されます。展開されたディレクトリの中に OpenAM の WAR ファイルが含まれているため、この WAR ファイルを利用します。

```
$ ls opt/osstech/share/openam14/openam.war
opt/osstech/share/openam14/openam.war
```

7.6 OpenAM WAR ファイルのディプロイ

OpenAM の WAR ファイルを Tomcat の webapps ディレクトリにコピーします。

```
$ cp openam.war {TOMCATDIR}/webapps/
```

7.7 Tomcat の起動

Tomcat を起動します。

```
$ export LANG="en_US.UTF-8"
$ systemctl start osstech-tomcat
```

OSSTech Tomcat 以外のアプリケーションサーバーを利用する場合は、文字化けを防ぐために環境変数 LANG に “en_US.UTF-8” を設定してください。

7.8 初期設定の開始

Tomcat が起動したら、ブラウザーで以下の URL にアクセスします。

- http://openam01.example.co.jp:8080/openam/

「設定オプション画面」が表示されます。この画面から OpenAM の初期設定を行います。

8 コンテキスト名の変更

本章では OpenAM のコンテキスト名（デフォルト: openam）を変更する方法を説明します。デフォルトの名称から変更したい場合は「Tomcat の起動」の前に本章の作業を実施ください。

8.1 server.xml の変更

コンテキスト名の変更は、`/opt/osstech/etc/tomcat` ディレクトリ以下にある server.xml にて行います。「`deployIgnore="openam"`」と「変更したい名称の定義」を追加します。

```
<Host name="localhost"  appBase="webapps"
       unpackWARs="true" autoDeploy="true"
       deployIgnore="openam">

        <Context path="/[変更したい名称]" docBase="openam"/>
</Host>
```

下記に example に変更する場合を示します。

```
<Host name="localhost"  appBase="webapps"
       unpackWARs="true" autoDeploy="true"
       deployIgnore="openam"> <!-- この定義を追加 -->

        <!-- openam から example に変える定義を追加 -->
        <Context path="/example" docBase="openam"/>
</Host>
```

この設定を行うと、OpenAM のアクセスは全て下記の通りとなります。

- http://openam01.example.co.jp:8080/example/

弊社ドキュメントはデフォルトの openam を想定しておりますので適宜読み替えてください

9 OpenLDAP スキーマ拡張

本章では OpenAM のデータストアとして OSSTech 版 OpenLDAP を利用する場合に必要なスキーマファイルのインストール手順について説明します。作業は OSSTech 版 OpenLDAP がインストールされているサーバーで行います。

9.1 準備

パッケージのインストールは、root ユーザーのみに許可されていますので、su コマンドで root ユーザーになります。

```
$ su -
Password: root のパスワードを入力（ 画面には表示されません ）
```

9.2 RPM パッケージのインストール

rpm コマンドを使用して、別途提供された osstech-openam-ldapschema パッケージをインストールします。

```
# rpm -ivh osstech-openam-ldapschema-x.x-x.elx.noarch.rpm
```

9.3 スキーマの有効化

/opt/osstech/etc/openldap/slapd.conf に下記の定義を追加し、インストールした OpenAM 用のスキーマファイルを読み込むように設定します。

```
include /opt/osstech/etc/openldap/schema/openam.schema
include /opt/osstech/etc/openldap/schema/saml2.schema
```

設定変更後、OpenLDAP を再起動します。

```
# systemctl restart osstech-slapd
```

10 OpenAM アップデート時の留意点

本章では OpenAM アップデート時の留意点について説明します。

なお、14.0 から 14.5 へは直接アップデート可能です。14.0 -> 14.1 -> 14.2 -> 14.5 と段階を踏んでアップデートする必要はありません。

10.1 OpenAM 14.1 より前のバージョンからアップデート

OpenAM 14.1 からログイン画面に表示される画像のロゴファイルのファイル名と画面サイズが変更されています。カスタマイズでロゴファイルを変更されている場合、「パッケージのアップデート」で以下の警告が表示されます。

```
Cleaning up / removing...
   2:osstech-openam14-14.0.0-xx.elx   warning: /opt/osstech/share/tomcat/webap
ps/openam/XUI/images/osstech-xui-login.png saved as /opt/osstech/share/tomcat/
webapps/openam/XUI/images/osstech-xui-login.png.rpmsave
```

この警告が表示された場合、パッケージのアップデート後に次の対応が必要です。

1. ロゴファイルの反映

```
# cd /opt/osstech/share/tomcat/webapps/openam/XUI/images
# mv osstech-xui-login.png.rpmsave openam-xui-login-logo.png
```

2. ThemeConfiguration.js ファイルの確認

/opt/osstech/share/tomcat/webapps/openam/XUI/config/ThemeConfiguration.js ファイルの loginLogo の src: と height: と width: を確認し、必要に応じて修正します。

```
    loginLogo: {
         // The URL of the image.
        src: "images/openam-xui-login-logo.png", <-- このファイル名であること
        // The title attribute used on <img> tags.
        title: "OSSTech",
        // The alt attribute used on <img> tags.
        alt: "OSSTech",
        // The height of the logo as a CSS length.
        height: "◯◯ px",   <-- カスタマイズロゴ画像の縦の長さであること
        // The width of the logo as a CSS length.
```

```
        width: "◯◯ px"      <-- カスタマイズロゴ画像の横の長さであること
    },
```

10.2 OpenAM 14.2 より前のバージョンからアップデート

OpenAM 14.2 では web.xml のサーブレットマッピングが変更されています。過去の脆弱性対応などで web.xml を変更している場合、「パッケージのアップデート」で以下の警告が表示されます。

```
Updating / installing...
   1:osstech-openam14-14.2.0-0.elx    warning: /opt/osstech/share/tomcat/webap
ps/openam/WEB-INF/web.xml created as /opt/osstech/share/tomcat/webapps/openam/
WEB-INF/web.xml.rpmnew
```

この警告が表示された場合、パッケージのアップデート後に次の対応が必要です。

1. 現在の web.xml のバックアップ

```
# mkdir -p /root/backup/webapps
# cd /opt/osstech/share/tomcat/webapps/openam/WEB-INF
# cp web.xml /root/backup/webapps
```

2. web.xml を最新のパッケージのものに差し替える

```
# mv web.xml.rpmnew web.xml
```

3. web.xml にカスタマイズ内容を反映する

脆弱性対応以外のカスタマイズがある場合は web.xml を修正してカスタマイズを反映してください。

10.3 OpenAM 14.5 より前のバージョンからアップデート

OpenAM 14.5 から SAML のポリシー保護機能の設定方法が変更されています。 1 号機のアップデート中に 2 号機の SAML のポリシー保護機能が無効になってしまうため、SAML のポリシー保護機能を有効にしている場合は「ローリングアップデート」を行うことができません。SAML のポリシー保護機能を有効にしている 2 台構成の OpenAM をアップデートする際は、OpenAM 両機の Tomcat を停止してからアップデートを行う必要があります。

SAML のポリシー保護機能を有効にしているかどうかは、OpenAM 管理コンソールの「連携」タブより対象の IdP をクリックし、「高度」タブに存在する「IDP アダプタクラス」設定をご確認ください。「IDP アダプタクラス」に「`jp.co.osstech.oam.saml2.plugins.PolicyCheckIDPAdapter`」が設定されている場合、ポリシー保護機能が有効化されています。

10.4 OpenAM 14.5.0-39 以降へのアップデート

OpenAM 14.5.0-39 から RHEL9 系及び RHEL8 系環境の OpenAM は OpenJDK 21 で動作するよう変更されました。

OpenJDK 21 で OpenAM を動作させるためには環境変数「JAVA_HOME」で OpenJDK 21 のディレクトリを指定し、更に OpenAM の動作に必要な JVM オプションを指定する必要があります。Tomcat を使用する場合、JVM オプションは環境変数「CATALINA_OPTS」により指定します。

OpenAM 14.5.0-39 以降の OpenAM 14 パッケージの RPM (osstech-openam14) には OpenJDK 21 での動作に必要な JAVA_HOME 及び CATALINA_OPTS の設定が行われた設定ファイル openam.conf が含まれており、以下のパスにインストールされます。

- /opt/osstech/etc/tomcat/tomcat.conf.d/openam.conf

10.4.1 RPM パッケージ標準構成の場合

OpenAM 14 パッケージをインストールしていて、かつ OpenAM が OSSTech Tomcat 上で動作している環境の場合、OSSTech Tomcat は openam.conf を使用します。そのため OpenAM を OpenJDK 21 で動作させるために JAVA_HOME 及び CATALINA_OPTS の設定を行う必要はありません。

ただし、設定変更により openam.conf を変更している場合、「パッケージのアップデート」で以下の警告が表示されます。

```
Updating / installing...
   1:osstech-openam14-14.5.0-xx.elx    warning: /opt/osstech/etc/tomcat/tomcat
.conf.d/openam.conf created as /opt/osstech/etc/tomcat/tomcat.conf.d/openam.co
nf.rpmnew
```

この警告が表示された場合、パッケージのアップデート後に次の対応が必要です。

1. 現在の openam.conf のバックアップ

```
# mkdir -p /root/backup/tomcat
# cd /opt/osstech/etc/tomcat/tomcat.conf.d
# cp openam.conf /root/backup/tomcat
```

2. openam.conf を最新のパッケージのものに差し替える

```
# mv openam.conf.rpmnew openam.conf
```

3. openam.conf に設定変更の内容を反映する

openam.conf に独自の変更がある場合は openam.conf を修正して変更内容を反映してください。

10.4.2 WAR ファイルをデプロイしている場合

OpenAM 14 パッケージに含まれる openam.conf を使用しない環境の場合、OpenAM を OpenJDK 21 で動作させるために JAVA_HOME 及び JVM オプションの設定が必要です。指定する必要がある JVM オプションは以下の通りです。

- `--add-opens=java.base/java.lang=ALL-UNNAMED`
- `--add-opens=java.rmi/sun.rmi.transport=ALL-UNNAMED`
- `--add-exports java.base/sun.security.tools.keytool=ALL-UNNAMED`
- `--add-exports java.base/sun.security.util=ALL-UNNAMED`
- `--add-exports java.base/sun.security.x509=ALL-UNNAMED`
- `--add-exports java.management/sun.management=ALL-UNNAMED`
- `--add-exports java.xml/com.sun.org.apache.xerces.internal.dom=ALL-UNNAMED`
- `--add-exports java.xml/com.sun.org.apache.xerces.internal.jaxp=ALL-UNNAMED`
- `--add-exports java.xml/com.sun.org.apache.xerces.internal.util=ALL-UNNAMED`

以下は Tomcat を使用している環境においてコマンドラインで指定する例です。

```
$ export CATALINA_OPTS="${CATALINA_OPTS} \
> --add-opens=java.base/java.lang=ALL-UNNAMED \
> --add-opens=java.rmi/sun.rmi.transport=ALL-UNNAMED \
> --add-exports java.base/sun.security.tools.keytool=ALL-UNNAMED \
> --add-exports java.base/sun.security.util=ALL-UNNAMED \
> --add-exports java.base/sun.security.x509=ALL-UNNAMED \
> --add-exports java.management/sun.management=ALL-UNNAMED \
```

```
> --add-exports java.xml/com.sun.org.apache.xerces.internal.dom=ALL-UNNAMED \
> --add-exports java.xml/com.sun.org.apache.xerces.internal.jaxp=ALL-UNNAMED \
> --add-exports java.xml/com.sun.org.apache.xerces.internal.util=ALL-UNNAMED"
```

その他、OS 起動時に実行されるスクリプト内や、Tomcat の起動スクリプト内などで CATALINA_OPTS を指定することもできます。

11 改版履歴

- 2019 年 12 月 13 日 リビジョン 1.0
  - 初版作成
- 2020 年 01 月 21 日 リビジョン 1.1
  - osstech-openam-ldapschema パッケージに関する記載を変更
- 2020 年 02 月 12 日 リビジョン 1.2
  - RHEL8 / CentOS8 に対応
  - RHEL7 / CentOS7 版のソフトウェア要件及び依存パッケージを変更
- 2020 年 03 月 11 日 リビジョン 1.3
  - インストール手順に Tomcat HTTP コネクターの設定変更を追記
- 2020 年 06 月 15 日 リビジョン 1.4
  - アップグレードの実行の分かり辛い URL の記載を変更
- 2020 年 10 月 16 日 リビジョン 1.5
  - Apache 経由でリクエストを受け付ける構成を追記
  - 起動/停止コマンドは systemctl を使用するよう変更
  - 他のドキュメントと合わせるため例示のホスト名を変更
  - ヒープサイズの記載を変更
- 2021 年 02 月 22 日 リビジョン 1.6
  - コンテキスト名の変更方法を修正
- 2021 年 05 月 28 日 リビジョン 1.7
  - パッケージのバージョン表記を変更
- 2021 年 09 月 03 日 リビジョン 1.8
  - OpenAM14.0 -> 14.1 アップデート時の注意点を追加
- 2022 年 05 月 02 日 リビジョン 1.9
  - 社名変更に伴う修正
  - 対応ブラウザーの章を追加
  - 14.2 より前のバージョンからアップデートする場合の注意点を追加
  - 初期設定画面及びアップグレード画面を更新
- 2022 年 12 月 19 日 リビジョン 1.10
  - OpenAM アップデート時の留意点を更新
  - アップグレード画面を更新
- 2023 年 02 月 09 日 リビジョン 1.11

  - OpenAM 2 台構成のアップデートの記載を変更
  - OpenAM 14.5 へのアップデート時の留意点を追加
- 2023 年 06 月 21 日 リビジョン 1.12
  - RHEL9 系 OS に対応
- 2024 年 04 月 25 日 リビジョン 1.13
  - コンテキスト名の変更で deployIgnore の定義が必要な点を強調
- 2024 年 06 月 18 日 リビジョン 1.14
  - RHEL9 及び RHEL8 系環境の OpenAM の動作に必要な OpenJDK を OpenJDK 21 に変更
  - RHEL9 及び RHEL8 系環境のパッケージ一式に含まれるファイル名とディレクトリ名を更新
  - OpenJDK のインストールコマンドで使用されているパッケージ名をヘッドレス版に変更
  - パッケージのアップデート手順に RHEL9 及び RHEL8 系環境の場合は OpenJDK 21 をインストールするよう追記
  - WAR ファイルのデプロイ手順に RHEL9 及び RHEL8 系環境の場合は Tomcat 用の CATALINA_OPTS の設定を行うよう追記
  - OpenAM 14.5.0-39 以降へアップデート時の留意点を追加
- 2024 年 08 月 09 日 リビジョン 1.15
  - WAR ファイルをデプロイしている場合に指定する必要がある JVM オプションの一覧にオプションを追加