

OpenAM サーバー（サイト構成）

構築手順書

オープンソース・ソリューション・テクノロジー(株)

文書番号:

作成日: 2012 年 5 月 24 日

リビジョン: 1.0

目次

1. 要旨	1
1.1 目的.....	1
1.2 作業概要.....	1
1.2.1 作業対象.....	1
1.2.2 作業内容.....	1
1.3 注意事項.....	1
2. システム構成	2
2.1 サーバー構成図.....	2
2.2 ソフトウェア構成.....	2
3. Linux OS 環境の構築	3
3.1 ファイアウォール設定.....	3
3.2 SELinux の無効化.....	3
3.3 ホスト名の名前解決確認.....	3
3.4 NTP 設定確認.....	4
4. パッケージの導入	5
4.1 インストール方法.....	5
4.1.1 OS 標準パッケージ.....	5
4.1.2 基本パッケージ.....	5
4.1.3 OpenAM 関連パッケージ.....	5
4.2 サーバプロセス自動起動設定.....	5
4.3 MANPATH の追加.....	6
4.4 Java 環境変数設定.....	6
5. OpenAM サーバー 1 号機の初期設定	7
5.1 起動.....	7
5.2 初期設定.....	7
6. OpenAM サーバー 2 号機の初期設定	10
6.1 起動.....	10
6.2 初期設定.....	10
7. OpenAM サーバーの設定(共通設定)	12
7.1 管理者ログイン.....	12
7.2 ロードバランサー設定(サイト構成).....	12
7.2.1 OpenAM サイト設定.....	12
8. 各種設定ファイル	14

8.1 OS 設定ファイル.....	14
8.1.1 ファイアウォール設定ファイル(/etc/sysconfig/iptables).....	14
9. 改版履歴	15

1. 要旨

本文書は、OpenAM サーバー(サイト構成)の構築手順書です。

1.1 目的

- OpenAM サーバー(サイト構成)を構築する

1.2 作業概要

1.2.1 作業対象

- OpenAM サーバー 1 号機
 - ホスト名 : oam1.example.co.jp
- OpenAM サーバー 2 号機
 - ホスト名 : oam2.example.co.jp
- ロードバランサー
 - lboam.example.co.jp

1.2.2 作業内容

1. OpenAM のインストールとサイト構成設定

1.3 注意事項

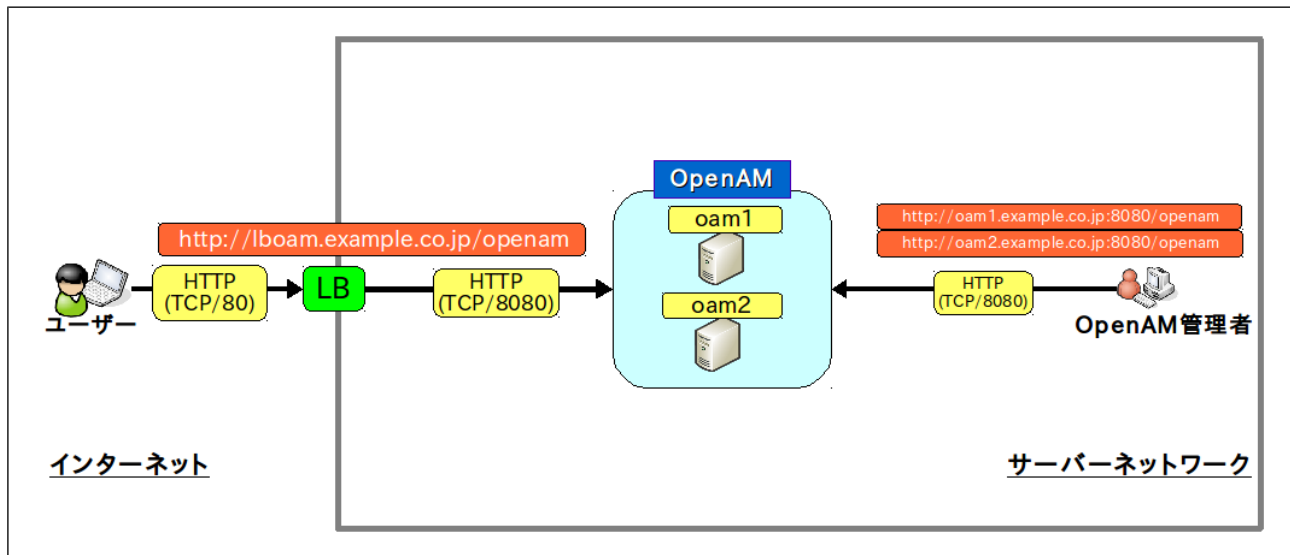
- サイト構成ではセッション情報の冗長化はされません。そのため、1号機にユーザーがログインした状態で1号機が停止し2号機のみ起動した状態となると、1号機にログインしたユーザーはログアウト状態となり、再びOpenAMへのログインが必要となります。
- 本文書は全ての通信を平文(HTTP)で行う前提です。

2. システム構成

本章では、シングルサインオンシステムのシステム構成について説明します。

2.1 サーバー構成図

本手順書で想定するサーバー構成です。



2.2 ソフトウェア構成

本システムで使用するソフトウェアの一覧です。

- OS
 - CentOS 5.7 x86_64
- OpenAM
 - OpenAM 9.5.4
- Java
 - Oracle JDK 1.6 Update 29
- アプリケーションサーバー
 - Tomcat 6.0.33

3. Linux OS 環境の構築

本章では、OpenAM サーバーが動作する Linux OS 環境の設定について説明します。設定は全ての OpenAM サーバーに対して設定します。手順は全ての OpenAM サーバーで共通です。

3.1 ファイアウォール設定

OpenAM サーバーに対する以下の通信を許可する必要があります。

- HTTP(TCP/8080)アクセス
- OpenAM 間の設定情報レプリケーション(OpenDS のレプリケーション)の通信

まず、ファイアウォールサービスを停止します。

```
# /sbin/service iptables stop
```

/etc/sysconfig/iptables を編集します。ファイルの内容は巻末をご参照ください。

ファイル作成後、パーミッションを設定します。

```
# chmod 600 /etc/sysconfig/iptables
# chown root:root /etc/sysconfig/iptables
```

ファイアウォールサービスを開始します。

```
# /sbin/service iptables start
```

OS 起動時に自動的にファイアウォールサービスが起動するように、以下のコマンドを実行します。

```
# /sbin/chkconfig iptables on
```

以上で完了です。

必要がなければ、ファイアウォールは無効でも問題ありません。

3.2 SELinux の無効化

OSSTech 版 OpenAM は SELinux が有効化された状態では動作しないため、SELinux を無効化します。
/etc/sysconfig/selinux に以下の内容を記述します。

```
SELINUX=disable
```

設定変更後、OS を再起動します。以上で完了です。

3.3 ホスト名の名前解決確認

本システムの全てのサーバー間で、FQDN によるホスト名の名前解決が可能であることを確認します。

- `/etc/hosts` に自ホスト(FQDN)が正確に記述されていることを確認します。
- `/etc/sysconfig/network` に自ホスト(FQDN)が正確に記述されていることを確認します。
- `/etc/resolv.conf` に DNS サーバーが登録されていることを確認します。
- DNS サーバー、もしくは、`/etc/hosts` ファイルにより各サーバーの名前解決が可能であることを確認します。

3.4 NTP 設定確認

NTP の設定がされていることを確認します。本システムは時刻が正確に合っていなければ正常に動作しない場合があります。そのため、NTP などにより時刻の同期を行うことが推奨されます。なお、NTP 設定は弊社の担当範囲外であるため、手順は割愛します。

4. パッケージの導入

本章では、OpenAM の構築に必要なパッケージのインストール手順について説明します。パッケージは全ての OpenAM サーバーにインストールします。手順は全ての OpenAM サーバーで共通です。

4.1 インストール方法

各パッケージをインストールします。

4.1.1 OS 標準パッケージ

まず、以下の OS 標準パッケージをインストールします。パッケージは OS インストール DVD のものを使用します。「xxx」はバージョン番号です。

```
# rpm -ivh httpd-2.2.3-xxx.rpm mod_ssl-xxx.rpm
```

4.1.2 基本パッケージ

弊社 RPM パッケージと依存関係にある基本パッケージをインストールします。

```
# rpm -ivh osstech-base-3.0-71.el5.noarch.rpm
```

4.1.3 OpenAM 関連パッケージ

OpenAM 関連パッケージをインストールします。

まず、JDK をインストールします。

```
# sh jdk-6u29-linux-x64-rpm.bin
```

コマンドラインのインストールウィザードが実行されます。続いて、Tomcat と OpenAM インストールします。

```
# rpm -ivh osstech-openam-9.5.4_RTM-0.el5.noarch.rpm ¥  
osstech-tomcat6-6.0.33-0.el5.noarch.rpm ¥
```

「\ (バックスラッシュ)」はコマンドラインの途中で改行を行なうために入力しています。「\」を入力せずに、全ての RPM ファイルを一行で指定することも可能です。

以上で完了です。

4.2 サーバプロセス自動起動設定

OS 起動時に各種サーバプロセスが自動的に起動するように設定します。

自動的に Apache HTTP Server が起動するように、以下のコマンドを実行します。

```
# /sbin/chkconfig httpd on
```

自動的に Tomcat が起動するように、以下のコマンドを実行します。

```
# /sbin/chkconfig osstech-tomcat6 on
```

以上で完了です。

4.3 MANPATH の追加

OSSTech 版 RPM は全て、/opt/osstech 以下にインストールされます。このディレクトリ配下のオンラインマニュアルを man コマンドで参照できるように、MANPATH を編集します。/etc/man.config に以下の行を追加します。

```
MANPATH /opt/osstech/share/man
```

4.4 Java 環境変数設定

Java 関連の環境変数が OS 全体で有効となるように設定します。

/etc/profile.d/java.sh を以下の内容で作成します。

```
JAVA_HOME="/usr/java/default"  
PATH=$JAVA_HOME/bin:$PATH  
export JAVA_HOME PATH
```

ファイルのパーミッションを設定します。

```
# chown root:root /etc/profile.d/java.sh  
# chmod 755 /etc/profile.d/java.sh
```

OS を再起動すると、OS 全体で設定が有効となります。

以上で完了です。

5. OpenAM サーバー 1 号機の初期設定

本章では、OpenAM サーバー 1 号機の構築手順について説明します。

5.1 起動

以下のコマンドを実行し、OpenAM を起動します。

```
[oaml]# /sbin/service osstech-tomcat6 start
```

5.2 初期設定

OpenAM の初期設定を行います。

1. 設定の開始

以下の URL にブラウザでアクセスすることにより OpenAM の設定を開始します。必ず完全修飾ドメイン名(FQDN)でアクセスして下さい。

- <http://oaml.example.co.jp:8080/openam>

設定オプション選択ページが表示されます。カスタム設定の「新しい設定の作成」を選択します。

2. 管理者ユーザーのパスワード設定

管理者ユーザー(amadmin)のパスワードを設定します。パスワードは8文字以上である必要があります。パスワードを入力し、「次へ」ボタンをクリックします。

3. サーバー設定

サーバー固有の設定情報を指定します。

- サーバー URL : OpenAM にアクセスするための URL です。通常はデフォルトのままで問題ありません。
- Cookie ドメイン : OpenAM が発行する Cookie のドメインを指定します。ここでは、「.example.co.jp」とします。
- プラットフォームロケール : デフォルトの「en_US」のままとします。
- 設定ディレクトリ : OpenAM の設定情報を保存するディレクトリを指定します。ログもここで指定したディレクトリに保存されます。デフォルトのままとします (/opt/osstech/share/tomcat6/openam と入力されているはずです)。

Cookie ドメインには、インストーラーがサーバーホスト名の FQDN の末尾から 2 番目のドットまでを抜き出したものが自動的に設定されています。ホスト名が「sso.example.co.jp」の場合「.co.jp」となりますが、「co.jp」ドメインの場合は Cookie ドメインに少なくとも 3 つのピリオドを含む必要があります (Cookie の仕様)。そのため、このような場合は適切なドメインに設定し直して下さい。例えば「sso.example.co.jp」の場合には「.example.co.jp」に設定し直します。設定が終わったら「次へ」ボタンをクリックします。

4. 設定データストアの設定

OpenAM の設定情報が保存される OpenDS (OpenAM 組込みの LDAP サーバー) の設定を行います。「最初のインスタンス」を選択します。

「設定データストア」は「OpenAM」を選択します。ポートやルートサフィックスは変更も可能ですが、設定データストア自体は OpenAM が内部的に参照するのみであるためデフォルトの設定で問題ありません。設定が終わったら「次へ」ボタンをクリックします。

5. ユーザーデータストアの設定

ユーザーデータストアとは、ユーザー情報を保存・参照するためのデータベースです。

OpenAM はユーザーデータストアとして Active Directory や OpenLDAP 等の外部データベースを使用することが可能です。これらは初期設定完了後に必要に応じて追加することが出来ます。

ここでは初期設定として「OpenAM のユーザーデータストア」を選択します。初期設定の段階では管理者ユーザーやデモユーザーが OpenAM のユーザーデータストアに保存されます。

設定が終わったら「次へ」ボタンをクリックします。

6. サイト設定

サイトとは OpenAM を 2 台以上構築する構成です。ロードバランサーの背後に配置された複数の OpenAM サーバー群をサイトと呼びます。この設定は初期設定完了後に実施するため、ここでは「いいえ」を選択して「次へ」ボタンをクリックします。

7. ポリシーエージェントのパスワード

デフォルトのポリシーエージェントのパスワードを設定します。ここでもパスワードは 8 文字以上にする必要があります、かつ管理者ユーザー (amadmin) のパスワードとは異なるものにする必要があります。設定が完了したら「次へ」ボタンをクリックします。

8. 設定の確認と反映

これまでの設定項目の一覧が表示されます。確認が済んだら「設定の作成」ボタンをクリックします。これにより設定がサーバーおよびデータストアに反映されます。

9. 設定の完了

設定の作成が完了すると「設定が完了しました」という画面が表示されます。

以上で初期設定は完了です。「ログインに進む」をクリックし、表示されるログイン画面から管理者ユーザー `amadmin` でログインできることを確認します。

6. OpenAM サーバー 2 号機の初期設定

本章では、OpenAM サーバー 2 号機の構築手順について説明します。

6.1 起動

以下のコマンドを実行し、OpenAM を起動します。

```
[oam2]# /sbin/service osstech-tomcat6 start
```

6.2 初期設定

OpenAM の初期設定を行います。

1. 設定の開始

以下の URL にブラウザでアクセスすることにより OpenAM の設定を開始します。必ず完全修飾ドメイン名(FQDN)でアクセスして下さい。

- <http://oam2.example.co.jp:8080/openam>

設定オプション選択ページが表示されます。カスタム設定の「新しい設定の作成」を選択します。

2. 管理者ユーザーのパスワード設定

管理者ユーザー(amadmin)のパスワードを設定します。1 号機と同じパスワードを入力し、「次へ」ボタンをクリックします。

3. サーバー設定

サーバー固有の設定情報を指定します。

- サーバー URL : OpenAM にアクセスするための URL です。通常はデフォルトのままで問題ありません。
- Cookie ドメイン : OpenAM が発行する Cookie のドメインを指定します。ここでは、「.example.co.jp」とします。
- プラットフォームロケール : デフォルトの「en_US」のままとします。
- 設定ディレクトリ : OpenAM の設定情報を保存するディレクトリを指定します。ログもここで指定したディレクトリに保存されます。デフォルトのままとします (/opt/osstech/share/tomcat6/openam と入力されているはずです)。

4. 設定データストアの設定

1号機に2号機を追加します。

- 「既存の配備に追加しますか」をチェックします。
- 「サーバー URL」に1号機の URL である「`http://oam1.example.co.jp:8080/openam`」を指定します。

「サーバー URL」を入力すると自動的に画面が更新され、「新しい OpenAM インスタンスのポート設定」、「既存の OpenAM インスタンスはレプリケーション用に設定されていません。次のポートが使用されます」というメッセージと、各種ポート番号が表示されます(ポートは自動的に検出・割り当てが行なわれます)。ここに表示されたポートが、設定データストアである OpenDS のレプリケーションに使用されます。これらのポートは OpenAM サーバー間での通信に使用されるため、ファイアウォール設定などを行なう場合はポート番号を控えておきます。デフォルト設定のまま、「次へ」ボタンをクリックします。

5. サイト設定

この設定は初期設定完了後に実施するため、ここでは「いいえ」を選択して「次へ」ボタンをクリックします。

6. 設定の確認と反映

これまでの設定項目の一覧が表示されます。確認が済んだら「設定の作成」ボタンをクリックします。

7. 設定の完了

設定の作成が完了すると「設定が完了しました」という画面が表示されます。

以上で初期設定は完了です。「ログインに進む」をクリックし、表示されるログイン画面から管理者ユーザー `amadmin` でログインできることを確認します。

7. OpenAM サーバーの設定(共通設定)

OpenAM の初期設定が完了した後に、シングルサインオンのための設定を行います。

7.1 管理者ログイン

OpenAM の各種設定を行う際は以下の URL にアクセスし、管理者アカウントでログインします。

- 1号機 : `http://oam1.example.co.jp:8080/openam`
- 2号機 : `http://oam2.example.co.jp:8080/openam`

上記 URL からログインして表示される画面を「管理コンソール」と呼びます。

7.2 ロードバランサー設定 (サイト構成)

サイト構成の設定です。ロードバランサー経由で OpenAM にアクセスするための設定手順について説明します。

7.2.1 OpenAM サイト設定

サイトとは OpenAM を 2 台以上構築する構成です。ロードバランサーの背後に配置された複数の OpenAM サーバー群をサイトと呼びます。ここではサイトを構成する手順を説明します。設定作業は 1 号機に対して行います。

1. OpenAM 管理コンソールの「設定」 → 「サーバーおよびサイト」を開きます。
2. 「サイト」の「新規」をクリックします。
3. 「名前」にサイト名を入力します。ここでは、「site1」と入力します。
4. 「プライマリ URL」にロードバランサーの URL を入力します。ここでは、「`http://lboam.example.co.jp/openam`」と入力します。URL の末尾に「/(スラッシュ)」をつけない点にご注意ください。「プライマリ URL」の末尾の「/(スラッシュ)」は OpenAM の内部処理で自動的に付与されるため、ここで「/(スラッシュ)」を入力すると正常に動作しません。
5. 画面右上の「了解」ボタンをクリックします。
6. 「サーバーおよびサイト」画面に戻ります。
7. 続いて、作成したサイトに実サーバーを登録します。「サーバー」の一覧にあるサーバー名のうち一つをクリックします(ここでは、1号機をクリックしたとします)。
8. 「サイト」 → 「親サイト」から、先程作成した「site1」を選択し、画面右上の「保存」ボタンをクリックします。

9. 「サーバーおよびサイト」画面に戻り、「サイト」の「割り当てられたサーバー」に「site1」を親サイトとして設定したサーバーが表示されていることを確認します。
10. 「サーバーおよびサイト」画面の「サーバー」の一覧にある他のサーバーに対しても同様の設定を行います。

以上で完了です。

8. 各種設定ファイル

各種設定ファイルを記載します。コメント類は省略し、パスワードは伏せ字にしています。「1号機」、「2号機」などの記載がないものは、全てのOpenAMサーバーで共通となります。

8.1 OS 設定ファイル

8.1.1 ファイアウォール設定ファイル(/etc/sysconfig/iptables)

関連部分のみ抜粋します。

```
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:RH-Firewall-1-INPUT - [0:0]
-A INPUT -j RH-Firewall-1-INPUT
-A FORWARD -j RH-Firewall-1-INPUT
(省略)
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 8080 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp -s 1号機の IP アドレス -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp -s 2号機の IP アドレス -j ACCEPT
(省略)
-A RH-Firewall-1-INPUT -j REJECT --reject-with icmp-host-prohibited
COMMIT
```

9. 改版履歴

- 2012 年 5 月 24 日 OSSTech 野村 健太郎
 - 初版作成