

OpenAM エージェント

インストールガイド



オープンソース・ソリューション・テクノロジー(株)

作成日: 2011 年 12 月 9 日

リビジョン: 1.4

目次

1. 概要	1
1.1 対象 OpenAM のバージョン.....	1
1.2 導入パッケージ一覧(RPM).....	1
2. 事前準備	2
2.1 ホスト名の名前解決.....	2
3. Apache Web Agent (Linux) のインストール	3
3.1 インストール条件.....	3
3.2 エージェントプロファイル作成.....	3
3.3 エージェント設定.....	4
3.4 エージェントインストール手順.....	4
3.5 エージェントアンインストール手順.....	8
4. 改版履歴	10

1. 概要

本書は OpenAM の各種 Agent のインストールガイドです。

1.1 対象 OpenAM のバージョン

本書では、エージェントと連携する OpenAM として、以下のバージョンを想定しています。

- OpenAM: OSSTech OpenAM Enterprise 9.5.x RTM

1.2 導入パッケージ一覧(RPM)

導入するパッケージ(RPM)の一覧です。ファイル名のうち、「OS」には OS の略称とメジャーバージョン番号、「arch」にはアーキテクチャ名が入ります。

- osstech-base-3.0-X.el5.noarch.rpm
- osstech-openam-agent-apache22-3.0.x.OS.arch.rpm

※「x」にはバージョン番号が入ります。

2. 事前準備

本章では、OpenAM エージェント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クッキーをドメインに対して設定します。また、エージェントと OpenAM 間の通信が発生する際には、エージェントは OpenAM が稼働するホストの FQDN を使用してアクセスします。そのため、クライアント、エージェント稼働ホスト、OpenAM サーバー間のアクセスは完全修飾ドメイン名(FQDN)で行う必要があります(注1)。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「sso.example.co.jp」として説明します。

(注1) : IP アドレス等の完全修飾ドメイン名以外でアクセスがあった場合には、OpenAM は完全修飾ドメイン名を使って自分自身にリダイレクトを行います。

3. Apache Web Agent (Linux) のインストール

本章では、Apache Web Agent (Linux 向け)のインストール手順を説明します。

3.1 インストール条件

エージェントをインストールする環境として、以下の環境を想定しています。

- OS : Red Hat Enterprise Linux 5、6、CentOS 5、6
- Apache HTTP Server 2.2
- JDK 6

3.2 エージェントプロファイル作成

エージェントをインストールする前に、OpenAM 側でエージェント設定(エージェントプロファイル)を事前に作成しておきます。

1. 以下の URL にアクセスし、OpenAM に管理者ユーザーでログインします。

`http://sso.example.co.jp:8080/openam`

2. 「アクセス制御」→「レルム名」→「エージェント」→「Web」を選択します。

3. 「エージェント」の「新規」をクリックします。

4. 各項目を入力します。

- a) 「名前」 : エージェントプロファイルの名前を入力します(例として、“apache22”と入力したものとします)。
- b) 「パスワード」 : エージェントの認証を行なうためのパスワードを入力します。ここで入力したパスワードは、エージェントをインストールする際に入力する必要があります。
- c) 「設定」 : 「集中」を選択します。
- d) 「サーバー URL」 : OpenAM の URL を入力します。ポート番号も指定してください。
- e) 「エージェント URL」 : エージェントの URL を入力します。ポート番号も指定してください。

5. 「作成」をクリックします。

以上で完了です。

3.3 エージェント設定

Apache Web Agent の基本設定について説明します。

1. OpenAM 管理コンソールの「アクセス制御」 → 「レルム」の対象レルム → 「エージェント」 → 「Web」 → 対象のエージェントを開きます。
2. 「グローバル」画面の以下のオプションを変更します。これらのオプションは Apache Web Agent では対応していないため無効にします。
 - 「プロファイル」 → 「通知を有効」：無効（有効のチェックをはずす）
 - 「一般」 → 「エージェントのデバッグファイルローテーション」：無効（有効のチェックをはずす）
 - 「監査」 → 「ローカル監査ログのローテーション」：無効（有効のチェックをはずす）
3. 画面右上の「保存」をクリックして設定を保存します。
4. 「OpenAM サービス」画面の以下のオプションを変更します。
 - 「ポリシークライアントサービス」 → 「SSO キャッシュポーリング期間」：1（分）
5. 画面右上の「保存」をクリックして設定を保存します。

以上で完了です。

3.4 エージェントインストール手順

Apache Web Agent (Linux 32bit 版)のインストール手順を説明します。なお、64bit 版でもインストール手順は同様の手順となります。

まず、Apache HTTP Server (httpd)を停止します。

```
# /sbin/service httpd stop
```

エージェントが OpenAM と通信する際に使用するパスワードをファイルに記述します。パスワードファイルはエージェントインストール時にのみ必要であり、インストール後は削除してもかまいません。パスワードファイルにはパスワードを平文で記述します。パスワードファイルは一行で記述し、改行コードを含まないものである必要があります。echo コマンドの“-n” オプションや tr コマンドを使用してパスワードファイルを生成します。

```
# echo -n "password" > passwd
```

もしくは

```
# vim passwd
(パスワードを記述して保存)
# tr -d '\n' < passwd
```

以下のようなファイルとなります(末尾に改行コードを含みません)。

```
password
```

以上でパスワードファイルの作成は完了です。記述したパスワードはエージェントインストール時に暗号化されてエージェントの設定ファイルに保存されます。続いて、エージェントのインストールを行います。

まず、RPMをインストールします(「X」の部分にはバージョン番号が入ります)。

```
# rpm -ivh osstech-base-3.0-X.el5.noarch.rpm osstech-openam-agent-apache22-X_RTM-X.el5.i386.rpm
```

次に、エージェントに含まれるインストーラを実行してインストールを行います。

```
# cd /opt/osstech/share/openam-agent-apache22/bin
# ./agentadmin --install
Please read the following License Agreement carefully:

[Press <Enter> to continue...] or [Enter n To Finish]
n      # 「n」を入力

Do you completely agree with all the terms and conditions of this License
Agreement (yes/no): [no]: yes      # 「yes」を入力
```

Apache HTTP Server の設定ファイルが存在するディレクトリのパスを入力します。

```
Enter the complete path to the directory which is used by Apache Server to
store its configuration Files. This directory uniquely identifies the
Apache Server instance that is secured by this Agent.
[ ? : Help, ! : Exit ]
Enter the Apache Server Config Directory Path [/opt/apache22/conf]: /etc/httpd/conf
```

OpenAM のURLを入力します。

```
Enter the URL where the OpenAM server is running. Please include the
deployment URI also as shown below:
(http://opensso.sample.com:58080/opensso)
[ ? : Help, < : Back, ! : Exit ]
OpenAM server URL: http://sso.example.co.jp:8080/openam
```

エージェントが稼働する Apache HTTP Server のURLを入力します。必ず、ポート番号(「:80」の部分)も指定してください。

```
Enter the Agent URL as shown below: (http://agent1.sample.com:1234)
[ ? : Help, < : Back, ! : Exit ]
Agent URL: http://agent.example.co.jp:80
```

事前に OpenAM 側で作成しておいた、エージェントプロファイルのプロファイル名を入力します。

```
Enter the Agent profile name
[ ? : Help, < : Back, ! : Exit ]
Enter the Agent Profile name: apache22
```

エージェントのパスワードファイルを指定します。

```
Enter the path to a file that contains the password to be used for identifying
the Agent.
[ ? : Help, < : Back, ! : Exit ]
Enter the path to the password file: /opt/osstech/etc/openam-agent-apache22/passwd
```

これまで入力したパラメーターの確認メッセージが表示されます。問題がない場合は「1」を選択し Enter を入力します。

```
-----
SUMMARY OF YOUR RESPONSES
-----
Apache Server Config Directory : /etc/httpd/conf
OpenAM server URL : http://sso.example.co.jp:8080/openam
Agent URL : http://agent.example.co.jp:80
Agent Profile name : apache22
Agent Profile Password file name : /opt/osstech/etc/openam-agent-apache22/passwd

Verify your settings above and decide from the choices below.
1. Continue with Installation
2. Back to the last interaction
3. Start Over
4. Exit
Please make your selection [1]:
```

インストールログが表示されます。

```
Creating directory layout and configuring Agent file for Agent_002
instance ...DONE.

Reading data from file /opt/osstech/etc/openam-agent-apache22/passwd and encrypting
it ...DONE.

Generating audit log file name ...DONE.
```

```
Creating tag swapped OpenSSOAgentBootstrap.properties file for instance
Agent_001 ...DONE.

Creating a backup for file /etc/httpd/conf/httpd.conf ...DONE.

Adding Agent parameters to
/opt/osstech/etc/openam-agent-apache22/Agent_001/config/dsame.conf file ...DONE.

Adding Agent parameters to /etc/httpd/conf/httpd.conf file ...DONE.

SUMMARY OF AGENT INSTALLATION
-----
Agent instance name: Agent_001
Agent Bootstrap file location:
/opt/osstech/etc/openam-agent-apache22/Agent_001/config/OpenAMAgentBootstrap.properties
Agent Configuration Tag file location
/opt/osstech/etc/openam-agent-apache22/Agent_001/config/OpenAMAgentConfiguration.properties
Agent Audit directory location:
/opt/osstech/etc/openam-agent-apache22/Agent_001/logs/audit
Agent Debug directory location:
/opt/osstech/etc/openam-agent-apache22/Agent_001/logs/debug

Install log file location:
/opt/osstech/etc/openam-agent-apache22/installer-logs/audit/install.log

Thank you for using OpenAM Policy Agent
```

以上でエージェントのインストールは完了です。

Apache HTTP Server (httpd)を起動します。

```
# /sbin/service httpd start
```

必要に応じて、パスワードファイルを削除します。

```
# rm /opt/osstech/etc/openam-agent-apache22/passwd
```

Apache HTTP Server は既にエージェントにより保護されているため、この状態(何もポリシーを設定していない状態)でアクセスすると、「403 Forbidden」となるはずです。

3.5 エージェントアンインストール手順

Apache Web Agent のアンインストール手順を説明します。

エージェントインストールディレクトリに移動し、agentadmin コマンドに「--uninstall」オプションを付加して実行します。

```
# cd /opt/osstech/share/openam-agent-apache22/bin
# ./agentadmin --uninstall
```

Apache HTTP Server の設定ファイルが存在するディレクトリのパスを入力します。

```
*****
Welcome to the OpenSSO Policy Agent for Apache Server.
*****

Enter the complete path to the directory which is used by Apache Server to
store its configuration Files. This directory uniquely identifies the
Apache Server instance that is secured by this Agent.
[ ? : Help, ! : Exit ]
Enter the Apache Server Config Directory Path [/opt/apache22/conf]: /etc/httpd/conf
```

確認メッセージが表示されます。問題がない場合は「1」を選択し Enter を入力します。

```
-----
SUMMARY OF YOUR RESPONSES
-----

Apache Server Config Directory : /etc/httpd/conf/

Verify your settings above and decide from the choices below.
1. Continue with Uninstallation
2. Back to the last interaction
3. Start Over
4. Exit
Please make your selection [1]:
```

アンインストールログが表示されます。

```
Deleting the config directory
/opt/osstech/share/openam-agent-apache22/Agent_002/config ...DONE.

Removing Agent parameters from /etc/httpd/conf/httpd.conf file ...DONE.

Uninstall log file location:
/opt/osstech/share/openam-agent-apache22/installer-logs/audit/uninstall.log
```

Thank you for using OpenSSO Policy Agent

以上で完了です。

4. 改版履歴

- 2011 年 03 月 23 日
 - OSSTech OpenAM パッケージ版として作成（リビジョン 1.0）
- 2011 年 04 月 11 日
 - Apache Web Agent のアンインストール手順を追記
- 2011 年 09 月 22 日
 - パスワードファイルの書式について説明を追記
- 2011 年 10 月 14 日
 - Apache Web Agent のエージェントプロファイルの設定を追記
- 2011 年 12 月 9 日
 - パスワードファイルに関する説明を追記
- 2012 年 3 月 26 日
 - バージョンの記述を修正