OpenAM OAuth 認証モジュール

設定手順書

オープンソース・ソリューション・テクノロジ(株)

作成者: 辻口 鷹耶
作成日: 2012 年 4 月 24 日
リビジョン: 1.0

目次

1. はじめに

本文書は OpenAM10.0 の新機能である OAuth 認証モジュールの設定手順について記載したものです。

1.1 OpenAM の対象バージョン

本文書では以下のバージョンで動作を確認しています。

- OpenAM10.0

1.2 対象 OAuth プロバイダ

本文書では以下の OAuth プロバイダを対象としています。

- Facebook

2. 要旨

2.1 OAuth 認証モジュールの概要

Oauth 認証モジュールは OAuth プロバイダに登録ずみのアカウントで OpenAM の認証を行う機能を提供します。また、OAuth で認可された情報を OpenAM のデータストアの情報にマッピングすることで、OAuth アカウントと OpenAM アカウントとを照合するだけではなく、アカウントを自動生成することも可能です。

2.2 設定手順

OAuth 認証モジュールは下記の手順で設定します。OAuth プロバイダによってアカウント登録の方法や OpenAM での設定内容は異なります。

1. OAuth アカウントの登録
2. OAuth アプリケーションの登録
3. OAuth 認証モジュール作成
4. OAuth 認証設定

3. Facebook

以下に Facebook と連携させるための設定方法を記載します。

3.1 OAuth アカウントの登録

Facebook にアプリケーションを登録し、クライアント ID 等を取得するには、まず Facebook のアカウント登録が必要です。

1. Focebook のログインサイトにアクセスし、アカウント登録を行います。

   http://www.facebook.com/

3.2 OAuth アプリケーションの登録

Facebook にアプリケーションを登録し、アプリケーションの ID とキーを取得します。

※本手順は 2012/4/10 時点のものです。

1. 『3.1OAuth アカウントの登録』で作成したアカウントにログインしている状態で Facebook のディベロッパーサイトのアプリケーション登録ページにアクセスします。

   https://developers.facebook.com/apps

2. ページ右上の「＋新しいアプリケーションの作成」ボタンを押下します
3. 表示されるダイアログで「App Name」と「App Namespace」を入力し、「続行」ボタン を押下します

   「App Name」と「App Namespace」は以降の設定に関与しないため、適当な名称でかまいません。

4. 表示されるダイアログで表示されている文字を入力し、『送信』を押下します
5. 基本設定画面で「アプリのドメイン」、「サイト URL」を入力して保存します

   「サイト URL」には OpenAM の URL を設定します。本設定では「アプリのドメイン」に OpenAM サーバーの FQDN を設定しています。

   以上でアプリケーションの登録は終了です。

※※注意※※

- Facebook の場合、作成直後のアカウントでアプリケーションの登録はできないようです
- アカウントの認証が済んでいない場合、携帯電話のメールアドレスを利用したワンタイムパスワード認証が必要です

3.3 OAuth 認証モジュール作成

OpenAM の管理コンソールで OAuth 認証モジュールを作成します。また、デフォルトの認証サービスに設定します。

1. OpenAM の管理コンソールにログインします
2. 認証設定画面を開きます

   [アクセス制御タブ]ー[(対象のレルム)]ー[認証タブ]
3. 「モジュールインスタンス」セクションで「新規」ボタンを押下します
4. 「名前」に facebook と入力し、「タイプ」に OAuth2.0 を選択して「了解」ボタンを押下します

   以上で OAuth 認証モジュールの作成は終了です

3.4 OAuth 認証設定

Oauth 認証モジュールに Facebook と連携するための設定を行います。なお、デフォルトで既に Facebook と連携する設定が行われているため、多くの項目は変更する必要がありません。

本手順では OpenAM のデータストアに Facebook ユーザが存在した場合に認証を許可する設定を行います。(ユーザが一致するかどうかはメールアドレスで判断します)

設定項目の意味やその他の動作設定については「4 参考」参照してください。

No	パラメータ名	設定値
1	ClientID	「3.2OAuth アプリケーションの登録」で登録した Facebook アプリケーションの「App ID/App Key」を入力する
2	Client Secret	Facebook アプリケーションの「App Secret」を入力する。
3	Authentication Endpoint URL	https://www.facebook.com/dialog/oauth (デフォルト)
4	Access Token Endpoint URL	https://graph.facebook.com/oauth/access_token (デフォルト)
5	User Profile Service URL	https://grapth.facebook.com/me (デフォルト)
6	Scope	email,read-stream (デフォルト)
7	Proxy URL	「https://[OpenAM サーバーの FQDN]:[ポート]/openam/oauth2c/OAuthProxy.jsp」
8	Account Mapper	(デフォルト)

No	パラメータ名	設定値
9	Account Mapper Configuration	email=mail
10	Attribute Mapper	(デフォルト)
11	Attribute Mapper Configuration	last_name=sn email=mail first_name=givenname name=cn
12	Save attribute in the session	有効
13	Email attribute in OAuth2 Response	email
14	Create account if it does not exist	無効
15	Prompt for password setting and activation code	無効
16	Map to anonymous user	無効
17	Anonymous User	anonymous (デフォルト)
18	OAuth 2.0 Provider logout service	http://www.facebook.com/logout.php (デフォルト)
19	Logout options	Prompt (デフォルト)

SMTP 関連の設定は「Create account if it does not exist」及び「Prompt for password setting and activation code」を有効にした場合のみ利用される。今回は特に設定しない。

3.5 動作確認

1. 認証モジュールに facebook を指定して OpenAM にアクセスします

   https://[openam サーバーの FQDN]:[ポート番号]/openam/UI/Login?module=facebook

2. 表示される facebook のログイン画面でメールアドレス及びパスワードを入力します
3. 確認画面でアプリケーションを許可します
4. 認証後の画面（OpenAM のユーザ画面）が表示されます

4. 参考

4.1 OAuth 認証モジュール パラメーター一覧

No	パラメータ名	説明
1	ClientID	OAuth プロバイダがクライアント(OpenAM)を識別する ID。
2	Client Secret	ClientID に対応するパスワード。
3	Authentication Endpoint URL	OAuth 認可サーバーの認可コードを発行する URL。
4	Access Token Endpoint URL	OAuth 認可サーバーのアクセストークンを発行する URL。
5	User Profile Service URL	OAuth アカウントのユーザプロファイルを提供する URL。
6	Scope	ユーザプロファイルの要求範囲。
7	Proxy URL	認可サーバーで認可後にリダイレクトされる URL。OpenAM の場合は下記の URL となる。 「https://[OpenAM サーバーの FQDN]:[ポート]/openam/oauth2c/OAuthProxy.jsp」
8	Account Mapper	Oauth アカウントを OpenAM アカウントにマッピングするクラス。特に条件や変換が必要ない場合にはデフォルトのクラスを使用する。
9	Account Mapper Configuration	Oauth アカウントと OpenAM アカウントの一致条件を指定する。条件が複数ある場合、1つでも一致すれば一致と判定される。 設定方法は、[OAuth 属性]=[OpenAM 属性]
10	Attribute Mapper	OAuth 属性を OpenAM 属性にマッピングするクラス。特に条件や変換が必要ない場合にはデフォルトのクラスを使用する。
11	Attribute Mapper Configuration	OAuth 属性と OpenAM 属性の対応表。 設定方法は、[OAuth 属性]=[OpenAM 属性]
12	Save attribute in the session	OAuth 属性をセッションに保存するかどうかを指定する。基本は有効。
13	Email attribute in OAuth2 Response	アクティベーションコードを送信するメールアドレス。OAuth 属性のうち、メールアドレスに該当する属性を設定する。

No	パラメータ名	
14	Create account if it does not exist	有効にすると、OpenAM のデータソースに OAuth アカウントが存在しない場合に自動でユーザを作成する。
15	Prompt for password setting and activation code	ユーザ自動作成時にパスワードの設定が可能。パスワード入力後は 13 で指定した OAuth アカウントのメールアドレスにアクティベーションコードが送信される。
16	Map to anonymous user	有効にすると、OpenAM に OAuth アカウントが存在しない場合に匿名ユーザとして認証される。
17	Anonymous User	匿名ユーザとして認証される場合に利用する OpenAM ユーザアカウント。
18	OAuth 2.0 Provider logout service	OAuth プロバイダのログアウトサービス URL。
19	Logout options	OpenAM のログアウト時に OAuth サービスのログアウトの動作を設定する。
20	Mail Server Gateway implementation class	メールを送信するクラス。通常はデフォルトのクラスを使用する。
21	SMTP host	SMTP サーバー。
22	SMTP port	SMTP のポート。
23	SMTP User Name	SMTP のユーザ名。
24	SMTP User Password	SMTP のユーザ名に対応するパスワード。
25	SMTP SSL Enabled	有効にすると、SMTP で SSL を有効にする。
26	SMTP From address	送信者のアドレス。
27	Authentication Level	認証レベル。

4.2 認証ケース毎の設定方法

OAuth 認証モジュールは複数の認証ケースが想定されています。

4.2.1 Case1 OpenAM にアカウント無い場合はエラーとする

OpenAM のデータストアに OAuth のアカウントが必要です。存在しない場合はエラーにします。

「3.4OAuth 認証設定」で示した設定となります。

4.2.2 Case2 OpenAM にアカウントが無い場合も認証する

OAuth で認証されていれば、OpenAM にデータストアに存在しない場合でも認証を許可します。

OAuth 認証モジュールの設定は Case1 と同様です。ただし、認証コア設定でユーザプロファイルを無視する設定を行うする必要があります。以下の手順で実施します。

1. [アクセス制御タブ]ー[(対象のレルム)]ー[認証タブ]
2. コアセクションの[すべてのコア設定]ボタンを押下します
3. User Profile セクションの「ユーザプロファイル」の設定に無視を選択して「保存ボタン」を押下します

4.2.3 Case3 OpenAM にアカウントが無い場合は作成する

OpenAM のデータストアに OAuth のアカウントが存在しない場合は、自動でアカウントを作成します。

OAuth 認証モジュールの設定について、Case 1との違いは以下の通りです。

- 「Create account if it does not exist」を有効にする

4.2.4 Case4 OpenAM にアカウントが無い場合は作成する(アクティベーション有り)

OpenAM のデータストアに OAuth のアカウントが存在しない場合は、アカウントを作成します。ただし、アカウント作成時にユーザにパスワード入力を促します。その後、メールで送信したアクティベーションコードが入力されることでアカウントを有効にします。

OAuth 認証モジュールの設定について、Case 1との違いは以下の通りです。

- 「Create account if it does not exist」を有効にする
- 「Prompt for password setting and activation code」を有効にする
- メール送信に関する設定を行う

  「SMTP host」、「SMTP port」、「SMTP User Name」、「SMTP User Password」、「SMTP SSL Enabled」、「SMTP From address」 を環境に合わせて設定する

4.2.5 Case5 OpenAM にアカウントが無い場合は匿名ユーザとして認証する

OpenAM のデータストアに OAuth のアカウントが存在しない場合は、匿名ユーザとして認証します。

OAuth 認証モジュールの設定について、Case 1との違いは以下の通りです。

- 「Map to anonymous user」を有効にする

4.3 参考文献

- OAuth2.0 Authentication (Facebook, Google, MSN, etc)

  ⇒OAuth 認証モジュールの概要(OpenAM wiki)

  https://wikis.forgerock.org/confluence/display/openam/OAuth+2.0+Authentication+%28Facebook,+Google,+MSN,+etc%29

- Configuring the OAuth 2.0 Authentication module

  ⇒OAuth 認証モジュールの設定ガイド

  https://wikis.forgerock.org/confluence/download/attachments/14942413/OAuth20_config.pdf?version=1&modificationDate=1322216637000

5. 改版履歴

- 2012 年 4 月 24 日　　辻口鷹耶
  - 新規作成