OpenShift Dedicated 4

アイデンティティープロバイダーの設定

アイデンティティープロバイダーの設定

Last Updated: 2021-09-27

OpenShift Dedicated 4 アイデンティティープロバイダーの設定

アイデンティティープロバイダーの設定

Enter your first name here. Enter your surname here.
Enter your organisation's name here. Enter your organisational division here.
Enter your email address here.

法律上の通知

概要

アイデンティティープロバイダーを設定して、ユーザーがクラスターにアクセスするためにログインする方法を決定します。

目次

第1章 アイデンティティープロバイダーの設定

OpenShift Dedicated クラスターの作成後に、アイデンティティープロバイダーを設定して、ユーザーがクラスターにアクセスする方法を決定する必要があります。

1.1. アイデンティティープロバイダーについて

OpenShift Dedicated には、ビルトイン OAuth サーバーが含まれます。開発者および管理者は OAuth アクセストークンを取得して、API に対して認証します。管理者は、クラスターのインストール後に、OAuth をアイデンティティープロバイダーを指定するように設定できます。アイデンティティープロバイダーを設定すると、ユーザーはログインし、クラスターにアクセスできます。

1.1.1. サポートされるアイデンティティープロバイダー

以下の種類のアイデンティティープロバイダーを設定できます。

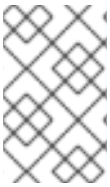
アイデンティティープロバイダー	詳細
GitHub または GitHub Enterprise	**github** アイデンティティープロバイダーを、GitHub または GitHub Enterprise の OAuth 認証サーバーに対してユーザー名とパスワードを検証するように設定します。
GitLab	**gitlab** アイデンティティープロバイダーを、GitLab.com またはその他の GitLab インスタンスをアイデンティティープロバイダーとして使用するように設定します。
Google	**google** アイデンティティープロバイダーを、Google の OpenID Connect 統合を使用して設定します。
LDAP	**ldap** アイデンティティープロバイダーを、単純なバインド認証を使用して LDAPv3 サーバーに対してユーザー名とパスワードを検証するように設定します。
OpenID Connect	**oidc** アイデンティティープロバイダーを、Authorization Code Flowを使用して OpenID Connect アイデンティティープロバイダーと統合するように設定します。
HTPasswd	単一の静的管理ユーザー用に **htpasswd** アイデンティティープロバイダーを設定します。問題のトラブルシューティングを行うには、ユーザーとしてクラスターにログインできます。

1.1.2. アイデンティティープロバイダーパラメーター

以下のパラメーターは、すべてのアイデンティティープロバイダーに共通するパラメーターです。

パラメーター	詳細
name	プロバイダー名は、プロバイダーのユーザー名にプレフィックスとして付加され、アイデンティティー名が作成されます。

パラメーター	詳細
mappingMethod	新規アイデンティティーがログイン時にユーザーにマップされる方法を定義します。以下の値のいずれかを入力します。 **claim** デフォルトの値です。アイデンティティーの推奨ユーザー名を持つユーザーをプロビジョニングします。そのユーザー名を持つユーザーがすでに別のアイデンティティーにマッピングされている場合は失敗します。 **lookup** 既存のアイデンティティー、ユーザーアイデンティティーマッピング、およびユーザーを検索しますが、ユーザーまたはアイデンティティーの自動プロビジョニングは行いません。これにより、クラスター管理者は手動で、または外部のプロセスを使用してアイデンティティーとユーザーを設定できます。この方法を使用する場合は、ユーザーを手動でプロビジョニングする必要があります。 **generate** アイデンティティーの推奨ユーザー名を持つユーザーをプロビジョニングします。推奨ユーザー名を持つユーザーがすでに既存のアイデンティティーにマッピングされている場合は、一意のユーザー名が生成されます。例: **myuser2**この方法は、OpenShift Dedicated のユーザー名とアイデンティティープロバイダーのユーザー名との正確な一致を必要とする外部プロセス (LDAP グループ同期など) と組み合わせて使用することはできません。 **add** アイデンティティーの推奨ユーザー名を持つユーザーをプロビジョニングします。推奨ユーザー名を持つユーザーがすでに存在する場合、アイデンティティーは既存のユーザーにマッピングされ、そのユーザーの既存のアイデンティティーマッピングに追加されます。これは、同じユーザーセットを識別して同じユーザー名にマッピングするアイデンティティープロバイダーが複数設定されている場合に必要です。



注記

mappingMethod パラメーターを **add** に設定すると、アイデンティティープロバイダーの追加または変更時に新規プロバイダーのアイデンティティーを既存ユーザーにマッピングできます。

1.2. GITHUB ID プロバイダーの設定

GitHub アイデンティティープロバイダーを、GitHub または GitHub Enterprise の OAuth 認証サーバーに対してユーザー名とパスワードを検証し、OpenShift Dedicated クラスターにアクセスするように設定します。OAuth は OpenShift Dedicated と GitHub または GitHub Enterprise 間のトークン交換フローを容易にします。

警告

GitHub 認証を設定することによって、ユーザーは GitHub 認証情報を使用して OpenShift Dedicated にログインできます。GitHub ユーザー ID を持つすべてのユーザーが OpenShift Dedicated クラスターにログインできないようにするために、アクセスを特定の GitHub 組織またはチームのユーザーに制限する必要があります。

前提条件

- OAuth アプリケーションは、GitHub 組織管理者によって GitHub 組織設定内に直接作成する必要があります。
- GitHub 組織またはチーム が GitHub アカウントに設定されている必要があります。

手順

1. OpenShift Cluster Manager (OCM) から、**Clusters** ページに移動し、アイデンティティープロバイダーを設定する必要のあるクラスターを選択します。
2. **Access control** タブをクリックします。
3. **Add identity provider** をクリックします。

注記

クラスターの作成後に表示される警告メッセージの **Add Oauth configuration** リンクをクリックして、アイデンティティープロバイダーを設定することもできます。

4. ドロップダウンメニューから **GitHub** を選択します。
5. アイデンティティープロバイダーの一意の名前を入力します。この名前は後で変更することはできません。
   - **OAuth callback URL** は提供されるフィールドに自動的に生成されます。これを使用して GitHub アプリケーションを登録します。

     ```
     https://oauth-openshift.apps.<cluster_name>.
     <cluster_domain>/oauth2callback/<idp_provider_name>
     ```

     以下は例になります。

     ```
     https://oauth-openshift.apps.example-openshift-cluster.com/oauth2callback/github/
     ```

6. アプリケーションを GitHub に登録します。
7. OpenShift Dedicated に戻り、ドロップダウンメニューからマッピング方法を選択します。ほとんどの場合、**Claim** が推奨されます。
8. GitHub から提供される **Client ID** および **Client secret** を入力します。
9. **hostname** を入力します。GitHub Enterprise のホステッドインスタンスを使用する場合は、ホスト名を入力する必要があります。
10. 任意手順: 認証局 (CA) ファイルを使用して、設定された GitHub Enterprise URL のサーバー証明書を検証できます。**Browse** をクリックして **CA ファイル** を見つけ、これをアイデンティティープロバイダーに割り当てます。
11. **Use organizations** または **Use teams** を選択し、アクセスを特定の GitHub 組織または GitHub チームに制限します。

12. アクセスを制限する組織またはチームの名前を入力します。**Add more** をクリックして、ユーザーが所属できる複数の組織またはチームを指定します。

13. **Confirm** をクリックします。

検証

- 設定されたアイデンティティープロバイダーが **Clusters** ページの **Access control** タブに表示されるようになりました。

1.3. GITLAB アイデンティティープロバイダーの設定

GitLab アイデンティティープロバイダーを、GitLab.com またはその他の GitLab インスタンスをアイデンティティープロバイダーとして使用するように設定します。

前提条件

- GitLab バージョン 7.7.0 から 11.0 を使用する場合、OAuth 統合を使用して接続します。GitLab バージョン 11.1 以降の場合、OAuth ではなく OpenID Connect (OIDC) を使用して接続します。

手順

1. OpenShift Cluster Manager (OCM) から、**Clusters** ページに移動し、アイデンティティープロバイダーを設定する必要のあるクラスターを選択します。

2. **Access control** タブをクリックします。

3. **Add identity provider** をクリックします。

注記

クラスターの作成後に表示される警告メッセージの **Add Oauth configuration** リンクをクリックして、アイデンティティープロバイダーを設定することもできます。

4. ドロップダウンメニューから **GitLab** を選択します。

5. アイデンティティープロバイダーの一意の名前を入力します。この名前は後で変更することはできません。

   - **OAuth callback URL** は提供されるフィールドに自動的に生成されます。この URL を GitLab に指定します。

     ```
     https://oauth-openshift.apps.<cluster_name>.
     <cluster_domain>/oauth2callback/<idp_provider_name>
     ```

     以下は例になります。

     ```
     https://oauth-openshift.apps.example-openshift-cluster.com/oauth2callback/gitlab/
     ```

6. GitLab に新規アプリケーションを追加します。

7. OpenShift Dedicated に戻り、ドロップダウンメニューからマッピング方法を選択します。ほとんどの場合、**Claim** が推奨されます。

8. GitLab から提供される **Client ID** および **Client secret** を入力します。
9. GitLab プロバイダーの **URL** を入力します。
10. オプション: 認証局 (CA) ファイルを使用して、設定された GitLab URL のサーバー証明書を検証できます。**Browse** をクリックして **CA ファイル** を見つけ、これをアイデンティティープロバイダーに割り当てます。
11. **Confirm** をクリックします。

検証

- 設定されたアイデンティティープロバイダーが **Clusters** ページの **Access control** タブに表示されるようになりました。

1.4. GOOGLE ID プロバイダーの設定

ユーザーが Google 認証情報で認証できるように Google アイデンティティープロバイダーを設定します。

警告

Google をアイデンティティープロバイダーとして使用することで、Google ユーザーはサーバーに対して認証されます。**hostedDomain** 設定属性を使用して、特定のホストドメインのメンバーに認証を限定することができます。

手順

1. OpenShift Cluster Manager (OCM) から、**Clusters** ページに移動し、アイデンティティープロバイダーを設定する必要のあるクラスターを選択します。
2. **Access control** タブをクリックします。
3. **Add identity provider** をクリックします。

注記

クラスターの作成後に表示される警告メッセージの **Add Oauth configuration** リンクをクリックして、アイデンティティープロバイダーを設定することもできます。

4. ドロップダウンメニューから **Google** を選択します。
5. アイデンティティープロバイダーの一意の名前を入力します。この名前は後で変更することはできません。
    - **OAuth callback URL** は提供されるフィールドに自動的に生成されます。この URL を Google に指定します。

```
https://oauth-openshift.apps.<cluster_name>.
<cluster_domain>/oauth2callback/<idp_provider_name>
```

以下は例になります。

```
https://oauth-openshift.apps.example-openshift-cluster.com/oauth2callback/github/
```

6. Google アイデンティティープロバイダーを、Google の OpenID Connect 統合 を使用して設定します。
7. OpenShift Dedicated に戻り、ドロップダウンメニューからマッピング方法を選択します。ほとんどの場合、**Claim** が推奨されます。
8. 登録済みの Google プロジェクトの **Client ID** と、Google が発行する **Client secret** を入力します。
9. ホストされたドメインを入力して、ユーザーを Google Apps ドメインに制限します。
10. **Confirm** をクリックします。

検証

- 設定されたアイデンティティープロバイダーが **Clusters** ページの **Access control** タブに表示されるようになりました。

1.5. LDAP アイデンティティープロバイダーの設定

LDAP アイデンティティープロバイダーを、単純なバインド認証を使用して LDAPv3 サーバーに対してユーザー名とパスワードを検証するように設定します。

前提条件

- LDAP アイデンティティープロバイダーを設定する場合は、設定済みの **LDAP URL** を入力する必要があります。設定される URL は、LDAP ホストと使用する検索パラメーターを指定する RFC 2255 URL です。URL の構文は以下のようになります。

```
ldap://host:port/basedn?attribute?scope?filter
```

URL コンポーネント	詳細
ldap	通常の LDAP の場合は、文字列 **ldap** を使用します。セキュアな LDAP (LDAPS) の場合は、代わりに **ldaps** を使用します。
host:port	LDAP サーバーの名前とポートです。デフォルトは、ldap の場合は **localhost:389**、LDAPS の場合は **localhost:636** です。
basedn	すべての検索が開始されるディレクトリーのブランチの DN です。これは少なくともディレクトリーツリーの最上位になければなりませんが、ディレクトリーのサブツリーを指定することもできます。

URL コンポーネント	詳細
attribute	検索対象の属性です。RFC 2255 はカンマ区切りの属性の一覧を許可しますが、属性をどれだけ指定しても最初の属性のみが使用されます。属性を指定しない場合は、デフォルトで **uid** が使用されます。使用しているサブツリーのすべてのエントリー間で一意の属性を選択することを推奨します。
scope	検索の範囲です。**one** または **sub** のいずれかを指定できます。範囲を指定しない場合は、デフォルトの範囲として **sub** が使用されます。
filter	有効な LDAP 検索フィルターです。指定しない場合、デフォルトは **(objectClass=*)** です。

検索の実行時に属性、フィルター、指定したユーザー名が組み合わされて以下のような検索フィルターが作成されます。

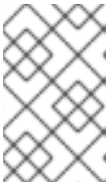
```
(&(<filter>)(<attribute>=<username>))
```

重要

LDAP ディレクトリーの検索に認証が必要な場合は、エントリー検索の実行に使用する **bindDN** と **bindPassword** を指定します。

手順

1. OpenShift Cluster Manager (OCM) から、**Clusters** ページに移動し、アイデンティティープロバイダーを設定する必要のあるクラスターを選択します。
2. **Access control** タブをクリックします。
3. **Add identity provider** をクリックします。



注記

クラスターの作成後に表示される警告メッセージの **Add Oauth configuration** リンクをクリックして、アイデンティティープロバイダーを設定することもできます。

4. ドロップダウンメニューから **LDAP** を選択します。
5. アイデンティティープロバイダーの一意の名前を入力します。この名前は後で変更することはできません。
6. ドロップダウンメニューからマッピング方法を選択します。ほとんどの場合、**Claim** が推奨されます。
7. **LDAP URL** を入力して、使用する LDAP 検索パラメーターを指定します。

8. オプション: **Bind DN** および **Bind password** を入力します。
9. LDAP 属性をアイデンティティーにマップする属性を入力します。
   - 値をユーザー ID として使用する **ID** 属性を入力します。**Add more** をクリックして、複数の ID 属性を追加します。
   - オプション: 表示名の値として使用する **Preferred username** 属性を入力します。**Add more** をクリックして、優先する複数のユーザー名属性を追加します。
   - オプション: メールアドレスの値として使用する **Email** 属性を入力します。**Add more** をクリックして、複数のメール属性を追加します。
10. オプション: **Show advanced Options** をクリックし、認証局 (CA) ファイルを LDAP アイデンティティープロバイダーに追加し、設定された URL のサーバー証明書を検証します。**Browse** をクリックして **CA ファイル** を見つけ、これをアイデンティティープロバイダーに割り当てます。
11. オプション: 高度なオプションで、LDAP プロバイダーを **非セキュア** にするよう選択できます。このオプションを選択すると、CA ファイルは使用できません。

重要

非セキュアな LDAP 接続（ldap:// またはポート 389）を使用している場合は、設定ウィザードで **で Insecure** オプションを確認する必要があります。

12. **Confirm** をクリックします。

検証

- 設定されたアイデンティティープロバイダーが **Clusters** ページの **Access control** タブに表示されるようになりました。

1.6. OPENID アイデンティティープロバイダーの設定

OpenID アイデンティティープロバイダーを、Authorization Code Flowを使用して OpenID Connect アイデンティティープロバイダーと統合するように設定します。

重要

OpenShift Dedicated の認証 Operator では、設定済みの OpenID Connect アイデンティティープロバイダーが OpenID Connect Discovery 仕様を実装する必要があります。

要求は、OpenID アイデンティティープロバイダーから返される JWT **id_token** から読み取られ、指定される場合は Issuer URL によって返される JSON から読み取られます。

1 つ以上の要求をユーザーのアイデンティティーを使用するように設定される必要があります。

また、どの要求をユーザーの推奨ユーザー名、表示名およびメールアドレスとして使用するか指定することができます。複数の要求が指定されている場合、値が入力されている最初の要求が使用されます。標準の要求は以下の通りです。

要求	詳細
preferred_username	ユーザーのプロビジョニング時に優先されるユーザー名です。**janedoe** などのユーザーを参照する際に使用する省略形の名前です。通常は、ユーザー名またはメールなどの、認証システムのユーザーのログインまたはユーザー名に対応する値です。
email	メールアドレス。
name	表示名。

詳細は、OpenID claim のドキュメント を参照してください。

前提条件

- OpenID Connect を設定する前に、OpenShift Dedicated クラスターで使用する Red Hat 製品またはサービスのインストール前提条件を確認してください。

手順

1. OpenShift Cluster Manager (OCM) から、**Clusters** ページに移動し、アイデンティティープロバイダーを設定する必要のあるクラスターを選択します。
2. **Access control** タブをクリックします。
3. **Add identity provider** をクリックします。

注記

クラスターの作成後に表示される警告メッセージの **Add Oauth configuration** リンクをクリックして、アイデンティティープロバイダーを設定することもできます。

4. ドロップダウンメニューから **OpenID** を選択します。
5. アイデンティティープロバイダーの一意の名前を入力します。この名前は後で変更することはできません。
   - **OAuth callback URL** は提供されるフィールドに自動的に生成されます。

     ```
     https://oauth-openshift.apps.<cluster_name>.
     <cluster_domain>/oauth2callback/<idp_provider_name>
     ```

     以下は例になります。

     ```
     https://oauth-openshift.apps.example-openshift-cluster.com/oauth2callback/openid/
     ```

6. Authorization Code Flow を使用して承認リクエストを作成します。
7. OpenShift Dedicated に戻り、ドロップダウンメニューからマッピング方法を選択します。ほとんどの場合、**Claim** が推奨されます。

8. OpenID から提供される **Client ID** および **Client secret** を入力します。
9. **Issuer URL** を入力します。これは、OpenID プロバイダーが発行者 ID としてアサートする URL です。URL クエリーパラメーターまたはフラグメントのない https スキームを使用する必要があります。
10. メールアドレスの値として使用する **Email** 属性を入力します。**Add more** をクリックして、複数のメール属性を追加します。
11. 優先するユーザー名の値として使用する **Name** 属性を入力します。**Add more** をクリックして、優先する複数のユーザー名を追加します。
12. 表示名の値として使用する **Preferred username** 属性を入力します。**Add more** をクリックして、複数の表示名を追加します。
13. オプション: **Show advanced Options** をクリックし、認証局 (CA) ファイルを OpenID アイデンティティープロバイダーに追加します。
14. オプション: 高度なオプションから、**追加のスコープ** を追加できます。デフォルトでは、**OpenID** の範囲が要求されます。
15. **Confirm** をクリックします。

検証

- 設定されたアイデンティティープロバイダーが **Clusters** ページの **Access control** タブに表示されるようになりました。

1.7. HTPASSWD アイデンティティープロバイダーの設定

HTPasswd アイデンティティープロバイダーを、クラスター管理者権限で単一の静的ユーザーを作成するように設定します。問題のトラブルシューティングを行うには、ユーザーとしてクラスターにログインできます。

手順

1. OpenShift Cluster Manager (OCM) から、**Clusters** ページに移動し、アイデンティティープロバイダーを設定する必要のあるクラスターを選択します。
2. **Access control** タブをクリックします。
3. **Add identity provider** をクリックします。

注記

クラスターの作成後に表示される警告メッセージの **Add Oauth configuration** リンクをクリックして、アイデンティティープロバイダーを設定することもできます。

4. **Identity Provider** ドロップダウンメニューから **HTPasswd** を選択します。
5. アイデンティティープロバイダーの **Name** フィールドに一意の名前を追加します。
6. 静的ユーザーに推奨されるユーザー名およびパスワードを使用するか、独自のユーザー名およびパスワードを作成します。

注記

この手順で定義した認証情報は、以下の手順で **Confirm** を選択した後に表示されません。認証情報を失った場合は、アイデンティティープロバイダーを再作成し、認証情報を再度定義する必要があります。

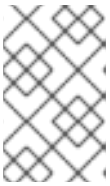
7. **Confirm** を選択し、HTPasswd アイデンティティープロバイダーおよびユーザーを作成します。
8. クラスターを管理する静的ユーザーにパーミッションを付与します。
   a. **Access control** ページの **Cluster administrative users** セクションで **Add user** を選択します。
   b. 前述の手順で定義したユーザー名を **User ID** フィールドに入力します。
   c. **Add user** を選択して、標準の管理者権限をユーザーに付与します。

注記

ユーザーは **dedicated-admins** グループに追加されます。

検証

- 設定されたアイデンティティープロバイダーが **Clusters** ページの **Access control** タブに表示されるようになりました。



注記

アイデンティティープロバイダーの作成後に、同期は通常 2 分以内に完了します。HTPasswd アイデンティティープロバイダーが利用可能になると、ユーザーとしてクラスターにログインできます。

1.8. クラスターへのアクセス

アイデンティティープロバイダーを設定したら、ユーザーは OpenShift Cluster Manager (OCM) からクラスターにアクセスできます。

前提条件

- クラスターが作成済みである。
- アイデンティティープロバイダーがクラスター用に設定されている。

手順

1. OpenShift Cluster Manager (OCM) で、アクセスするクラスターをクリックします。
2. **Open Console** をクリックします。
3. アイデンティティープロバイダーをクリックし、クラスターにログインするためのクレデンシャルを指定します。

検証

- クラスターにアクセスすると、OpenShift Dedicated クラスターのコンソールに移動します。