Generic OAuth Authentication

通用OAuth认证

 › [Administration](https://grafana.com/docs/grafana/latest/administration/) › [Authentication](https://grafana.com/docs/grafana/latest/auth/) › Generic OAuth

You can configure many different OAuth2 authentication services with Grafana using the generic OAuth2 feature. Examples:

你可以使用通用的OAuth2功能在Grafana中配置多个不同的OAuth2认证服务。

* [Auth0](https://grafana.com/docs/grafana/latest/auth/generic-oauth/#set-up-oauth2-with-auth0)
* [Azure AD](https://grafana.com/docs/grafana/latest/auth/azuread/)
* [BitBucket](https://grafana.com/docs/grafana/latest/auth/generic-oauth/#set-up-oauth2-with-bitbucket)
* [Centrify](https://grafana.com/docs/grafana/latest/auth/generic-oauth/#set-up-oauth2-with-centrify)
* [Okta](https://grafana.com/docs/grafana/latest/auth/okta/)
* [OneLogin](https://grafana.com/docs/grafana/latest/auth/generic-oauth/#set-up-oauth2-with-onelogin)

This callback URL must match the full HTTP address that you use in your browser to access Grafana, but with the prefix path of /login/generic\_oauth.

这个回调URL必须匹配你在浏览器中访问Grafana的完整HTTP地址，是/login/generic\_oauth的前缀。

You may have to set the root\_url option of [server] for the callback URL to be correct. For example in case you are serving Grafana behind a proxy.

你可能需要为了正确的回调URL去设置[server]的root\_url。例如你是服务Grafana背后的代理。

Example config:

[auth.generic\_oauth]

enabled = true

client\_id = YOUR\_APP\_CLIENT\_ID

client\_secret = YOUR\_APP\_CLIENT\_SECRET

scopes =

auth\_url =

token\_url =

api\_url =

allowed\_domains = mycompany.com mycompany.org

allow\_sign\_up = true

Bash

Set api\_url to the resource that returns [OpenID UserInfo](https://connect2id.com/products/server/docs/api/userinfo) compatible information.

设置api\_url去返回OpenID UserInfo的兼容信息。

Grafana will attempt to determine the user’s e-mail address by querying the OAuth provider as described below in the following order until an e-mail address is found:

Grafana会试图通过查询OAuth供应者去决定用户的邮箱地址，作为下面顺序中的描述，直到一个邮箱地址被发现：

1. Check for the presence of an e-mail address via the email field encoded in the OAuth id\_token parameter.

通过OAuth id\_token参数中编码的email字段,检查是否存在电子邮件地址

1. Check for the presence of an e-mail address using the [JMESPath](http://jmespath.org/examples.html) specified via the email\_attribute\_path configuration option. The JSON used for the path lookup is the HTTP response obtained from querying the UserInfo endpoint specified via the api\_url configuration option. **Note**: Only available in Grafana v6.4+.

使用规定的JMESPath如email\_attribute\_path配置项来检查是否存在电子邮件。用于路径查找的JSON，是HTTP响应从指定api\_url配置项中查询的UserInfo端获取到。注意：只在Grafana6.4及以后的版本可用。

1. Check for the presence of an e-mail address in the attributes map encoded in the OAuth id\_token parameter. By default Grafana will perform a lookup into the attributes map using the email:primary key, however, this is configurable and can be adjusted by using the email\_attribute\_name configuration option.

通过OAuth的id\_token参数中编码的attributes映射来检查是否存在电子邮件地址。默认Grafana会使用email:primary来执行一个attributes的映射查找，无论如何，这个是可配置的，并能使用email\_attribute\_name配置项调整。

1. Query the /emails endpoint of the OAuth provider’s API (configured with api\_url) and check for the presence of an e-mail address marked as a primary address.

查询OAuth后缀为/emails的供应者API（在api\_url中配置），并检查是否存在标记为主地址的电子邮件地址

1. If no e-mail address is found in steps (1-4), then the e-mail address of the user is set to the empty string.

如果不能在上面的步骤中找到电子邮件地址，那么用户的电子邮件地址会被设置为空字符串。

Grafana will also attempt to do role mapping through OAuth as described below.

Grafana也会按照如下所述的方法试图去做OAuth的角色映射。

Only available in Grafana v6.5+.

只在Grafana6.5版本后可用。

Check for the presence of a role using the [JMESPath](http://jmespath.org/examples.html) specified via the role\_attribute\_path configuration option. The JSON used for the path lookup is the HTTP response obtained from querying the UserInfo endpoint specified via the api\_url configuration option. The result after evaluating the role\_attribute\_path JMESPath expression needs to be a valid Grafana role, i.e. Viewer, Editor or Admin.

使用role\_attribute\_path配置项指定的JMESPath去检查是否存在角色。用于路径查找的JSON，是HTTP响应从指定api\_url配置项中查询的UserInfo端获取到。评估role\_attribute\_path的JMESPath表达式后的结果，需要作为Grafana的有效的角色，如Viewer,Editor或Admin.

See [JMESPath examples](https://grafana.com/docs/grafana/latest/auth/generic-oauth/" \l "jmespath-examples) for more information.

查看JMESPath例子来了解更多信息。

Set up OAuth2 with Auth0

使用Auth0来安装OAuth2

1. Create a new Client in Auth0

在Auth0中创建一个新的客户端

* + Name: Grafana

名字：Grafana

* + Type: Regular Web Application

类型：普通的网络应用

1. Go to the Settings tab and set:

跳到设置标签并设置

* + Allowed Callback URLs: https://<grafana domain>/login/generic\_oauth

允许回调URL：https://<grafana domain>/login/generic\_oauth

1. Click Save Changes, then use the values at the top of the page to configure Grafana:

点击保存修改，然后使用页面顶部的值来配置Grafana

[auth.generic\_oauth]

enabled = true

allow\_sign\_up = true

team\_ids =

allowed\_organizations =

name = Auth0

client\_id = <client id>

client\_secret = <client secret>

scopes = openid profile email

auth\_url = https://<domain>/authorize

token\_url = https://<domain>/oauth/token

api\_url = https://<domain>/userinfo

Bash

Set up OAuth2 with Bitbucket

用Bitbucket安装OAuth2

[auth.generic\_oauth]

name = BitBucket

enabled = true

allow\_sign\_up = true

client\_id = <client id>

client\_secret = <client secret>

scopes = account email

auth\_url = https://bitbucket.org/site/oauth2/authorize

token\_url = https://bitbucket.org/site/oauth2/access\_token

api\_url = https://api.bitbucket.org/2.0/user

team\_ids =

allowed\_organizations =

Bash

Set up OAuth2 with Centrify

使用Centrify安装OAuth2

1. Create a new Custom OpenID Connect application configuration in the Centrify dashboard.

在Centrify Dashboard中创建一个新的自定义的OpenID连接应用配置

1. Create a memorable unique Application ID, e.g. “grafana”, “grafana\_aws”, etc.

创建一个好记唯一应用ID，如grafana，grafana\_aws等

1. Put in other basic configuration (name, description, logo, category)

提交其他的基础配置（名字，描述，标志，分类）

1. On the Trust tab, generate a long password and put it into the OpenID Connect Client Secret field.

在Trust标签，在OpenID连接客户端机密字段中输入一个长的密码。

1. Put the URL to the front page of your Grafana instance into the “Resource Application URL” field.

将你的Grafana实例的前端页面URL输入到“Resource Application URL”字段中。

1. Add an authorized Redirect URI like <https://your-grafana-server/login/generic_oauth>

添加一个已认证的重定向URI，像<https://your-grafana-server/login/generic_oauth>

1. Set up permissions, policies, etc. just like any other Centrify app

安装权限，策略等正如其他的Centrify应用一样。

1. Configure Grafana as follows:

如下配置Grafana：

[auth.generic\_oauth]

name = Centrify

enabled = true

allow\_sign\_up = true

client\_id = <OpenID Connect Client ID from Centrify>

client\_secret = <your generated OpenID Connect Client Secret"

scopes = openid profile email

auth\_url = https://<your domain>.my.centrify.com/OAuth2/Authorize/<Application ID>

token\_url = https://<your domain>.my.centrify.com/OAuth2/Token/<Application ID>

api\_url = https://<your domain>.my.centrify.com/OAuth2/UserInfo/<Application ID>

Bash

Set up OAuth2 with OneLogin

使用OneLogin安装OAuth2

1. Create a new Custom Connector with the following settings:

使用下面的设置来创建一个新的自定义连接：

* + Name: Grafana

名字：Grafana

* + Sign On Method: OpenID Connect

登录方式：OpenID连接

* + Redirect URI: https://<grafana domain>/login/generic\_oauth

重定向URI：https://<grafana domain>/login/generic\_oauth

* + Signing Algorithm: RS256

签名算法：RS256

* + Login URL: https://<grafana domain>/login/generic\_oauth

登录URL：https://<grafana domain>/login/generic\_oauth

then:

然后：

1. Add an App to the Grafana Connector:

添加一个应用到Grafana连接：

* + Display Name: Grafana

显示名字：Grafana

then:

然后：

1. Under the SSO tab on the Grafana App details page you’ll find the Client ID and Client Secret.

在Grafana应用详情页面的SSO标签下，你能找到ClientID和Client机密。

Your OneLogin Domain will match the URL you use to access OneLogin.

你的OneLogin域名会匹配到你能登录到的OneLogin的URL。

Configure Grafana as follows:

如下配置Grafana：

[auth.generic\_oauth]

name = OneLogin

enabled = true

allow\_sign\_up = true

client\_id = <client id>

client\_secret = <client secret>

scopes = openid email name

auth\_url = https://<onelogin domain>.onelogin.com/oidc/2/auth

token\_url = https://<onelogin domain>.onelogin.com/oidc/2/token

api\_url = https://<onelogin domain>.onelogin.com/oidc/2/me

team\_ids =

allowed\_organizations =

Bash

JMESPath examples

JMESPath例子

To ease configuration of a proper JMESPath expression, you can test/evaluate expressions with custom payloads at <http://jmespath.org/>.

为了一个适当的JMESPath表达式，你能在<http://jmespath.org/>中使用自定义的payload来测试/评估表达式。

Role mapping

角色映射

**Basic example:**

**基本例子：**

In the following example user will get Editor as role when authenticating. The value of the property role will be the resulting role if the role is a proper Grafana role, i.e. Viewer, Editor or Admin.

在下面的例子中，用户会在认证时获得Editor的角色。如果角色是一个适当的Grafana角色，那么role属性的值会是Viewer，Editor或Admin。

Payload:

{

...

"role": "Editor",

...

}

JSON

Config:

role\_attribute\_path = role

Bash

**Advanced example:**

**进阶例子：**

In the following example user will get Admin as role when authenticating since it has a group admin. If a user has a group editor it will get Editor as role, otherwise Viewer.

在下面的例子中，admin组的用户会在认证时获取Admin角色。如果一个用户有Editor组，那么他会获取Editor角色，否则为Viewer。

Payload:

{

...

"info": {

...

"groups": [

"engineer",

"admin",

],

...

},

...

}

JSON

Config:

role\_attribute\_path = contains(info.groups[\*], 'admin') && 'Admin' || contains(info.groups[\*], 'editor') && 'Editor' || 'Viewer'

Bash