Connect invisionpowerboard and matrix chat using oauth

Nowadays every community needs a chat of some sort. And by nowadays I mean: it has actually always been like that. Some decades ago we used IRC. But the things have changed. Solutions need to be more accessible.

The context is this: we have an online forum community where members register and participate. The member account is based in the forum software. We want members to be able to join the chat without any more fuzz than necessary.

Here is what we are going to use:

- invisioncommunity - a well know board software to host online forums.
    - its OAuth API to connect the chat server, allowing users to login with the same account
- matrix chat, specifically:
    - synapse as the server (its the matrix reference homeserver)
    - element (previously called "riot") as web client

To be able to setup the OAuth connection the invisioncommunity, synapse and element services need to be accessible by https. I can recommend using let sencrypt certificates. But this guide does not explain this part. But the resulting apache config is shown below.

This configuration examples has the domains setup to:

- the forum reachable at `www.yourhostname.com`
- the matrix server at `matrix.yourhostname.com`
- the element web chat at `riot.yourhostname.com`

The tools allow you to host your own community without depending on other services or cloud solutions - but still using modern solutions.

Step 1: add an OAuth Application in invisioncommunity

Login into the AdminCP and add an OAuth application. Remember the *client identifier* and the *client secret*. The *client secret* can not be shown again - but it can be regenerated.

- Client Type: Custom Confidential OAuth Client
- Available Grant Types: Authorization Code
- Require PKCE for Authorization Code grant?: Not required
- Redirection URIs: https://matrix.yourhostname.com/_synapse/client/oidc/callback
- Authorization Prompt: Never
  this will allow your invisioncommunity members to just open the element chat, get redirected a few times, but then be already connected and online in the chat.
- Allow users to choose scopes? off
- Show in Account Settings? on
- Access Tokens: leave the defaults
- Scopes: profile and email. leave the defaults

Step 2: configure the OIDC provider

The official documentation contains more examples.

homeserver.yaml

```
oidc_providers:
  - idp_id: yourhostname
    idp_name: "Yourhostname.com Login"
    discover: false
    issuer: "https://www.hostname.com/"
    client_id: "changeme"
    client_secret: "secret_changeme_aswell"
    scopes: ["email", "profile"]
    authorization_endpoint: "https://www.yourhostname.com/oauth/authorize/"
    token_endpoint: "https://www.yourhostname.com/oauth/token/"
    userinfo_endpoint: "https://www.yourhostname.com/api/core/me"
    user_mapping_provider:
      config:
        subject_claim: "name"
        localpart_template: "{{ user.name }}"
        display_name_template: "{{ user.name }}"
        email_template: "{{ user.email }}"
```

Use the client_id and client_secret from step 1. Make sure the url's you use are all correct. The authorization_ token_ and userinfo_ endpoints are specific to the invisioncommunity software.

The user_mapping_provider configures the chat so the forum username is used as name in the chat.

After you change the homeserver.yaml you need to restart the service.

Step 3: configure the Element web chat for your community

Our goal here is to have a simple way for the forum users to use the chat - not hosting a chat solution for anyone interested. So the users are still managed in the invisioncommunity software. So in this configuration we will disable the registration and some other options.

config.json

```
{
    "default_server_config": {
        "m.homeserver": {
            "base_url": "https://matrix.yourhostname.com",
            "server_name": "matrix.yourhostname"
        }
    },
    "sso_immediate_redirect": true,
    "disable_custom_urls": true,
    "disable_guests": true,
    "disable_login_language_selector": true,
    "disable_3pid_login": true,
    "brand": "riot.yourhostname.com",
    "defaultCountryCode": "DE",
    "showLabsSettings": false,
    "features": {
        "feature_new_spinner": "labs",
        "feature_pinning": "labs",
        "feature_custom_status": "labs",
        "feature_custom_tags": "labs",
        "feature_state_counters": "labs"
    },
    "default_federate": false,
    "default_theme": "light",
    "welcomeUserId": "@riot-bot:matrix.org",
    "enable_presence_by_hs_url": {
        "https://matrix.org": false,
        "https://matrix-client.matrix.org": false,
        "https://matrix.yourhostname.com": true
    },
    "settingDefaults": {
        "breadcrumbs": true,
        "UIFeature.shareSocial": false,
        "UIFeature.registration": false,
        "UIFeature.passwordReset": false,
        "UIFeature.deactivate": false,
        "UIFeature.thirdPartyId": false
    },
    "jitsi": {
        "preferredDomain": "jitsi.riot.im"
    }
}
```

The default welcome screen is disabled, so users will not need to re-login or create an account. Users can't change their password or anything, as these things still happen in the invisioncommunity.

There you go! Chat is on! 👍

Configurations files

Docker configuration

Docker-compose file:

docker-compose.yaml

```
version: '3'

services:

  element:
    image: vectorim/element-web:v1.9.0
    restart: unless-stopped
    volumes:
      - ./element/config.json:/app/config.json
    depends_on:
      - synapse
    ports:
      - 28009:80

  synapse:
    image: matrixdotorg/synapse:v1.43.0
    restart: unless-stopped
    environment:
      - SYNAPSE_SERVER_NAME=matrix.yourhostname.com
      - SYNAPSE_REPORT_STATS=yes
      - UID=1006
      - GID=1020
    volumes:
      - ./data:/data
    depends_on:
      - db
    ports:
      - 28008:8008

  db:
    image: postgres:14.0
    environment:
      - POSTGRES_USER=synapse
      - POSTGRES_PASSWORD=synapseDBpassword
      - POSTGRES_INITDB_ARGS=--encoding=UTF-8 --lc-collate=C --lc-ctype=C
    volumes:
      - ./pgdata:/var/lib/postgresql/data
```

Notes:

- UID and GID are the user and group id of your linux user and group.
- adjust the synapse_server_name.
- make sure the exposed ports match the ones in the apache configuration.

Apache2 configuration

Site-Configuration. Requires SSL, Headers, Proxy.

```
<IfModule mod_ssl.c>
<VirtualHost *:443>
        SSLEngine on
        ServerAdmin admin@hostname.com
        ServerName matrix.hostname.com

        ErrorLog /var/log/apache2/matrix.hostname.com_error.log
        TransferLog /var/log/apache2/matrix.hostname.com_access.log

        RequestHeader set "X-Forwarded-Proto" expr=%{REQUEST_SCHEME}

        AllowEncodedSlashes NoDecode
        ProxyPreserveHost on
        ProxyPass /_matrix http://127.0.0.1:28008/_matrix nocanon
        ProxyPassReverse /_matrix http://127.0.0.1:28008/_matrix
        ProxyPass /_synapse/client http://127.0.0.1:28008/_synapse/client nocanon
        ProxyPassReverse /_synapse/client http://127.0.0.1:28008/_synapse/client

        Include /etc/letsencrypt/options-ssl-apache.conf
        SSLCertificateFile /etc/letsencrypt/live/0002/fullchain.pem
        SSLCertificateKeyFile /etc/letsencrypt/live/0002/privkey.pem
</VirtualHost>

<VirtualHost *:443>
        ServerAdmin admin@hostname.com
        ServerName riot.hostname.com

        ErrorLog /var/log/apache2/riot.hostname.com_error.log
        TransferLog /var/log/apache2/riot.hostname.com_access.log

        RequestHeader append "X-Frame-Options" "SAMEORIGIN"
        RequestHeader append "X-Content-Type-Options" "nosniff"
        RequestHeader append "X-XSS-Protection" "1; mode=block"
        RequestHeader append "Content-Security-Policy" "frame-ancestors 'none'"

        ProxyPreserveHost On
        ProxyPass / http://127.0.0.1:28009/
        ProxyPassReverse / http://127.0.0.1:28009/

        Include /etc/letsencrypt/options-ssl-apache.conf
        SSLCertificateFile /etc/letsencrypt/live/0002/fullchain.pem
        SSLCertificateKeyFile /etc/letsencrypt/live/0002/privkey.pem
</VirtualHost>

</IfModule>
```

If you end up in a redirect loop in the matrix server make sure the "ProxyPreserveHost on" statement in present.