Setting up an OAuth authentication server for a Grafana dashboard in an offline environment involves several steps. The process typically includes setting up an OAuth server (such as IdentityServer, Keycloak, or an alternative), configuring it with the necessary clients and scopes, and configuring Grafana to use this server for authentication. Here's a step-by-step guide:

**1. Set Up an OAuth Authentication Server**

**Option 1: Using IdentityServer**

**IdentityServer** is an open-source framework for implementing an OAuth2 and OpenID Connect server.

1. **Download and Install IdentityServer:**
   * You can use the IdentityServer templates for .NET if you're familiar with .NET development.
   * Alternatively, you can use the IdentityServer4 Docker image if you prefer Docker.
2. **Configure IdentityServer:**
   * Define the API resources, clients, and users in the Config.cs file.
   * Ensure the OAuth server is configured to run without internet access.

**Option 2: Using Keycloak**

**Keycloak** is another open-source identity and access management solution.

1. **Download and Install Keycloak:**
   * Download Keycloak from the official website.
   * Follow the installation instructions for your operating system.
2. **Configure Keycloak:**
   * Create a realm and define the clients and roles.
   * Ensure Keycloak is configured to run offline.

**2. Configure OAuth Clients and Scopes**

Regardless of the OAuth server you choose, you'll need to configure the clients and scopes.

1. **Create a Client for Grafana:**
   * Set the client ID and client secret.
   * Define the redirect URI to point to your Grafana instance (e.g., http://localhost:3000/login/generic\_oauth).
2. **Set Up Scopes and Roles:**
   * Define the necessary scopes and roles that Grafana will use for authorization.

**3. Configure Grafana to Use OAuth**

1. **Edit the Grafana Configuration:**
   * Locate the grafana.ini file, typically found in /etc/grafana/grafana.ini or the equivalent directory for your installation.
2. **Configure OAuth Settings:**

[auth.generic\_oauth]

enabled = true

name = OAuth

allow\_sign\_up = true

client\_id = your\_client\_id

client\_secret = your\_client\_secret

auth\_url = http://your-oauth-server/auth

token\_url = http://your-oauth-server/token

api\_url = http://your-oauth-server/userinfo

scopes = openid profile email

1. **Restart Grafana:**
   * After configuring the grafana.ini file, restart the Grafana service to apply the changes.

**4. Test the Configuration**

1. **Access the Grafana Dashboard:**
   * Open your web browser and navigate to your Grafana instance.
   * Click on the OAuth login option you configured.
2. **Authenticate:**
   * You should be redirected to your OAuth server's login page.
   * After logging in, you should be redirected back to Grafana with an authenticated session.

**5. Troubleshooting**

* **Check Logs:**
  + Both Grafana and your OAuth server will have logs that can help troubleshoot issues.
  + Ensure there are no network issues preventing communication between Grafana and the OAuth server.
* **Review OAuth Configuration:**
  + Verify client ID, client secret, and redirect URIs are correctly configured.

**Example: Using IdentityServer4 with Docker**

Here’s an example of setting up IdentityServer4 using Docker:

1. **Pull the Docker Image:**

docker pull identityserver/identityserver4

1. **Run the Docker Container:**

docker run -d -p 5000:80 --name my\_identity\_server identityserver/identityserver4

1. **Configure the Container:**
   * Connect to the running container and edit the configuration files to define clients, scopes, and users.

By following these steps, you should be able to set up an OAuth authentication server for Grafana in an offline environment. Make sure to adapt the configurations to fit your specific setup and security requirements.