Installing an OAuth authentication server on a Windows machine in an offline environment involves several steps, including setting up the environment, downloading necessary software and dependencies on an internet-connected machine, transferring them to the offline machine, and configuring the server. Below is a step-by-step guide using Keycloak as an example:

**Step 1: Prepare the Environment**

1. **Choose a Windows Machine:**
   * Select a Windows server or a suitable Windows PC that will host your OAuth server. Ensure it has the required specifications for running your OAuth server software.
2. **Install the Operating System:**
   * Ensure that Windows is installed and properly configured.

**Step 2: Download Necessary Software and Dependencies**

1. **Download Keycloak:**
   * From a machine with internet access, download the Keycloak server from the official Keycloak downloads page.
2. **Download JDK (Java Development Kit):**
   * Download the appropriate version of the JDK from [AdoptOpenJDK](https://adoptopenjdk.net/) or Oracle's website.
3. **Download Database Software:**
   * Download the necessary database software or JDBC driver if required. Keycloak supports databases like PostgreSQL, MySQL, etc.
4. **Download Required Dependencies:**
   * If Keycloak has other dependencies (like specific libraries or tools), download these as well. Check the documentation for any additional requirements.
5. **Transfer Files to the Offline Server:**
   * Use a USB drive or any other method to transfer the downloaded files to the offline Windows machine.

**Step 3: Install and Configure the Software**

1. **Install JDK:**
   * Transfer the JDK installation file to the offline server and install it:

plaintext

Copy code

Install the JDK by running the installer and following the instructions.

* + Set up environment variables:
    1. Right-click on 'This PC' or 'Computer' on the desktop or in File Explorer.
    2. Select 'Properties'.
    3. Click on 'Advanced system settings'.
    4. Click on 'Environment Variables'.
    5. Under 'System variables', click 'New' and add JAVA\_HOME with the path to the JDK (e.g., C:\Program Files\Java\jdk-xx).
    6. Find the 'Path' variable, select it, and click 'Edit'. Add %JAVA\_HOME%\bin.

1. **Install the Database:**
   * Install the database software. For example, if using PostgreSQL:

plaintext

Copy code

Run the PostgreSQL installer and follow the instructions to set up the database.

1. **Configure the Database:**
   * Set up the database for Keycloak. Open psql and run:

sql

Copy code

CREATE USER keycloak WITH PASSWORD 'password';

CREATE DATABASE keycloakdb;

GRANT ALL PRIVILEGES ON DATABASE keycloakdb TO keycloak;

1. **Install Keycloak:**
   * Extract the Keycloak server:

plaintext

Copy code

Unzip the Keycloak archive (keycloak-xx.zip) to a directory, e.g., `C:\keycloak`.

1. **Configure Keycloak:**
   * Update the Keycloak configuration files to point to your database. Edit standalone/configuration/standalone.xml or use environment variables:

xml

Copy code

<datasource>

<connection-url>jdbc:postgresql://localhost:5432/keycloakdb</connection-url>

<driver>postgresql</driver>

<username>keycloak</username>

<password>password</password>

</datasource>

**Step 4: Start and Test the OAuth Server**

1. **Start Keycloak:**
   * Open Command Prompt, navigate to the Keycloak bin directory, and run:

plaintext

Copy code

cd C:\keycloak\bin

standalone.bat

1. **Create Admin User:**
   * Open Command Prompt, navigate to the Keycloak bin directory, and run:

plaintext

Copy code

add-user-keycloak.bat -r master -u admin -p password

1. **Access Keycloak:**
   * Open a web browser on a machine that can access the server and navigate to http://localhost:8080/auth.
   * Log in with the admin credentials you created.
2. **Configure OAuth Clients and Users:**
   * Use the Keycloak admin console to configure OAuth clients, users, and roles as needed.

**Step 5: Secure and Maintain the Server**

1. **Secure the Server:**
   * Configure SSL/TLS for secure communication.
   * Set up firewalls and security settings to restrict access.
2. **Regular Backups:**
   * Ensure regular backups of the database and Keycloak configuration.
3. **Monitor and Update:**
   * Regularly monitor the server's health and apply offline updates as necessary.

By following these steps, you should be able to set up an OAuth authentication server on a Windows machine in an offline environment.