PAM – Installationsanleitung

Diese Anleitung gibt einen Überblick darüber, wie die Software “PAM” installiert und zur Verfügung gestellt werden kann. Folgende Voraussetzungen müssen erfüllt sein:

- Ein Server, welcher Unterstützung für Docker, sowie Docker Compose bietet
- Ein SSL-Zertifikat im PKCS12 (p12) Format, falls SSL-Support gewünscht ist
- Eine Microsoft Entra ID (Azure) OAuth2 Registrierung
- Zugriff auf den PAM-Quellcode

PAM ist als Docker-Container-App konzipiert, daher soll nur dieser Anwendungsfall in dieser Anleitung betrachtet werden. PAM basiert dabei auf einer Spring-Boot Anwendung und könnte daher auch ohne Docker betrieben werden.

Konfiguration von PAM:

Im PAM-Quellcode findet sich im Root-Verzeichnis die Datei “docker-compose.release.yml”. Diese Datei enthält sämtliche Konfigurationsoptionen, welche den PAM-Container konfigurieren können.

Diese sollen im Folgenden erklärt werden:

- *services.db.environment:*
  - *MYSQL_ROOT_PASSWORD*: Das Root-Passwort mit welchem der SQL-Container erstellt wird. Notwendig für spätere manuelle Zugriffe.
  - *MYSQL_PASSWORD*: Das Passwort, mit welchem PAM auf die Datenbank zugreifen kann.
  - *MYSQL_DATABASE*: Die Datenbank, welche automatisch für PAM erstellt wird.
  - *MYSQL_USER*: Benutzername für den PAM-User.
  - *MYSQL_TCP_PORT:* Der TCP-Port, unter welchem die Datenbank zur Verfügung gestellt wird.
- *services.app.environment:*
  - *MYSQL_PORT:* Der Port, mit welchem sich PAM mit einer Datenbank verbindet. Dieser muss mit *services.db.environment.MYSQL_TCP_PORT* übereinstimmen, falls keine externe Datenbank verwendet wird.
  - *MYSQL_HOST*: Der Hostname, unter dem PAM sich mit der Datenbank verbindet. Dieser muss mit *db* übereinstimmen, falls keine externe Datenbank verwendet wird.
  - *MYSQL_USER:* Der Benutzername, welcher für die Anmeldung an die Datenbank verwendet wird. Dieser muss mit *services.db.environment.MYSQL_USER* übereinstimmen, falls keine externe Datenbank verwendet wird.
  - *MYSQL_PASSWORD*: Das Passwort, welches für die Anmeldung an die Datenbank verwendet wird. Dieses muss mit *services.db.environment.MYSQL_PASSWORD* übereinstimmen, falls keine externe Datenbank verwendet wird.
  - *MYSQL_SCHEMA*: Das Datenbank-Schema, welches PAM in der Datenbank öffnet. Diese muss mit *services.db.environment.MYSQL_DATABASE* übereinstimmen, falls keine externe Datenbank verwendet wird.

- *AZURE_TENAT_ID*: Die Azure Tenat ID, welche PAM für die Verwendung von Microsoft OAuth2 verwenden soll. Diese kann in Microsoft Entra ID herausgefunden werden.
- *AZURE_CLIENT_ID:* Die Azure Client ID, welche PAM für die Verwendung von Microsoft OAuth2 verwenden soll. Diese kann in Microsoft Entra ID herausgefunden werden.
- *AZURE_CLIENT_SECRET:* Das Azure Client Secret, welches PAM für die Verwendung von Microsoft OAthu2 verwenden soll. Diese kann in Microsoft Entra ID herausgefunden werden.
- *SSL_ENABLE:* Wenn diese Option auf *true* gesetzt ist, verwendet PAM *https* statt *http*. Diese ist erforderlich, um Azure zu verwendet, falls PAM nicht hinter einer *https*-Proxy verwendet wird. Benötigt *services.app.environment.SSL_KEYSTORE_PATH, services.app.environment.SSL_KEYSTORE_PASSWORD* und *services.app.environment.SSL_KEYSTORE_ALIAS*, wenn der Wert auf *true* gesetzt ist. Um diese Option zu deaktivieren, muss der Wert auf *false* gesetzt werden.
- *SSL_KEYSTORE_PATH:* Der Pfad zum PKCS12 (Dateiendung: *p12*) verschlüsselten *X.509* Zertifikat, welches verwendet wird, um https zu aktivieren. Dieser Pfad gilt nur im Container für Ordner die unter *services.app.volumes* eingerichtet wurden.
- *SSL_KEYSTORE_PASSWORD:* Das Passwort für das PKCS12 verschlüsselte *X.509* Zertifikat.
- *SSL_KEYSTORE_ALIAS*: Der Name des Zertifikates aus dem PKCS12 Keystore, welches PAM für SSL verwenden soll.
- *AFTER_LOGOUT_URI*: Die URI zu welcher PAM einen Benutzer weiterleiten soll, wenn dieser die Logout-Funktion verwendet.
- *OID_READER*: Die ID der Microsoft Entra ID Sicherheitsgruppe, welche ein Nutzer haben muss, um die Rolle *Reader* zu erhalten.
- *OID_DESIGNER*: Die ID der Microsoft Entra ID Sicherheitsgruppe, welche ein Nutzer haben muss, um die Rolle *Designer* zu erhalten.
- *OID_ADMIN*: Die ID der Microsoft Entra ID Sicherheitsgruppe, welche ein Nutzer haben muss, um die Rolle *Admin* zu erhalten.

- *services.app.volumes*:
  - Hier können die Pfade eingegeben werden, welche im PAM-Container verfügbar sein sollen. Es empfiehlt sich hier einen Ordner anzugeben, um den PKCS12-Keystore verfügbar zu machen.

    Beispiel:
    Wenn auf dem Server der PKCS12 unter dem Pfad */home/pam/certs/keystore_pam.p12* aufzufinden ist, dann muss */home/pam/certs/:/certs* zu den *volumes* hinzugefügt werden, sowie *services.app.environment.SSL_KEYSTORE_PATH* auf */certs/keystore_pam.p12* gesetzt werden.
- *services.app.ports*:
  - Hier kann ein Port Mapping eingestellt werden.
    Folgende Beispielmöglichkeiten:
    "443:8080" PAM verwendet *https* und ist direkt unter Port 443 verfügbar.
    "80:8080" PAM verwendet *http* und ist direkt unter Port 80 verfügbar.

Starten und Updaten von PAM:

Nach Konfiguration von PAM kann der Container mit folgendem Befehl gestartet werden (dieser muss im Root-Ordner des PAM-Quellcodeverzeichnisses ausgeführt werden):

docker compose –f docker-compose.release.yml up –d

Hierdurch werden die notwendigen Container gestartet und PAM steht zur Verfügung. Zum Stoppen von PAM kann folgender Befehl verwendet werden (dieser muss im Root-Ordner des PAM-Quellcodeverzeichnisses ausgeführt werden):

docker compose –f docker-compose.release.yml down

Falls sich Änderungen am Quellcode ergeben und PAM geupdatet werden soll, muss PAM zunächst gestoppt werden. Danach kann das Container Image mit dem folgenden Befehl geupdatet werden (die Datenbank bleibt dabei erhalten):

docker compose –f docker-compose.release.yml build —no-cache

Danach kann PAM wieder gestartet werden.

Updaten von bpmn-js:

PAM verwendet bpmn-js als Library für die BPMN – Modellierung. Falls ein Update dieser Library gefordert ist, kann diese wie folgt geändert werden:
In den Dateien src/main/resources/templates/viewer.html und src/main/resources/templates/modeler.html alle Vorkommnisse von bpmn-js@15.1.3 suchen und die Version durch eine neue Version ersetzten. Achtung: Durch das Ändern der bpmn-js Version kann es zu Inkompatibilitäten kommen, welche Änderungen am Quellcode benötigen.