PAM Jump Server Installation

The purpose of this tutorial is to show how to install Jump servers and configure PAM using Docker compose, to use critical resources without knowing the password required.

Jump Server

> A jump server, jump host or jump box is a system on a network used to access and manage devices in a separate security zone. A jump server is a hardened and monitored device that spans two dissimilar security zones and provides a controlled means of access between them. (*)

Installation

1. Execute the Store YAML

```
version: '3.8'

services:
  pam-store:
    image: soffid/pam-store:1.4.36
    environment:
      JAVA_KEYSTORE: /opt/soffid/tomee/certificados/YOUR_soffid-pam-store.jks
      KEYSTORE_PASS: YOUR_KEYSTORE
    networks:
      - network
    volumes:
      - store-certificados:/opt/soffid/tomee/certificados
      - store-data:/opt/soffid/tomee/data

networks:
  network:
```

```
    name: YOUR_NETWORK
    driver: bridge

volumes:
  store-certificados:
    name: soffid-pam-certificados
  store-data:
    name: soffid-pam-store
```

Execute:

```
sudo docker compose up -d
```

2. Create a user in the Store to use it in the Launcher

Once, we are connected to the Store, we need to run a script to create the user. This script has two parameters, the user name, and the role. We have to type launcher in the role parameter.

```
docker exec YOUR_pam-store_CONTAINER /opt/soffid/tomee/bin/add-user.sh usuario-launcher launcher
```

Result:

```
/bin/bash: warning: setlocale: LC_ALL: cannot change locale (en_US.UTF-8)
Password: cccccc/Qul9NFIqQnDU73gYccccVHThyew7Qt8Hqpf0rEzVq1Ft7azccccccc
```

As a result of the script, we receive the password for the created user. This password will be needed later when we create the launcher container.

3. Create a user in the Store to use it in the Console

Once, we are connected to the Store, we need to run a script to create the user. This script has two parameters, the user name, and the role. We have to type console in the role parameter.

```
docker exec YOUR_pam-store_CONTAINER /opt/soffid/tomee/bin/add-user.sh usuario-console console
```

Result:

```
/bin/bash: warning: setlocale: LC_ALL: cannot change locale (en_US.UTF-8)
Password: asdadadasdads/Qul9NFIqQnDU73gYccccVHThyew7Qt8Hqpf0rEzVq1Ft7aadadadasd
```

As a result of the script, we receive the password for the created user. This password will be needed later when we configure PAM in the Soffid Console.

4. Execute the Launcher YAML

YAML example to create the Launcher using traefik as Ingress Controller

```
version: '3.8'

services:
  pam-launcher:
    image: soffid/pam-launcher:1.4.36
    environment:
      JAVA_KEYSTORE: /opt/soffid/tomee/certificados/YOUR_soffid-pam-launcher.jks
      KEYSTORE_PASS: YOUR_KESYSTORE
      STORE_SERVER: https://YOUR_pam-store_CONTAINER:8443
      STORE_USER: usuario-launcher
      STORE_PASSWORD: cccccc/Qul9NFIqQnDU73gYccccVHThyew7Qt8Hqpf0rEzVq1Ft7azccccccc
    ports:
      - "8082:8443"
    networks:
      - network
    volumes:
      - launcher-certificados:/opt/soffid/tomee/certificados
      - launcher-data:/opt/soffid/tomee/data

networks:
  network:
    name: YOUR_NETWORK
    driver: bridge

volumes:
  launcher-certificados:
    name: soffid-pam-certificados
  launcher-data:
    name: soffid-pam-launcher
```

Execute:

```
sudo docker compose up -d
```

5. Configure the Console

Privileged Account Session Recording

Be in mind that you need to download the latest image of the required Privileged Account Session Recording that you need depending on the protocol.

- soffid-pars-ssh
- soffid-pasr-rdp
- soffid-pasr-jdbc
- soffid-pasr-http
- soffid-pasr-https
- soffid-pasr-tn5250
- soffid-pasr-kube

To save a Web session you will need to add some parameters to the launcher system.properties (/opt/soffid/tomee/conf/system.properties)

Parameters to add:

```
SOFFID_PAM_PARAMS_http=--shm-size=1024m  --privileged -eVNCSERVER=yes
SOFFID_PAM_PARAMS_https=--shm-size=1024m  --privileged -eVNCSERVER=yes
```

(*) https://en.wikipedia.org/wiki/Jump_server

Revision #3
Created 6 August 2024 13:57:47 by pgarcia@soffid.com
Updated 6 August 2024 14:18:49 by pgarcia@soffid.com