PAM Monitoring

Monitoring and reporting

- Privileged accounts dashboard
- Search in PAM recordings
- Access logs
- Sessions
- System Monitoring

Privileged accounts dashboard

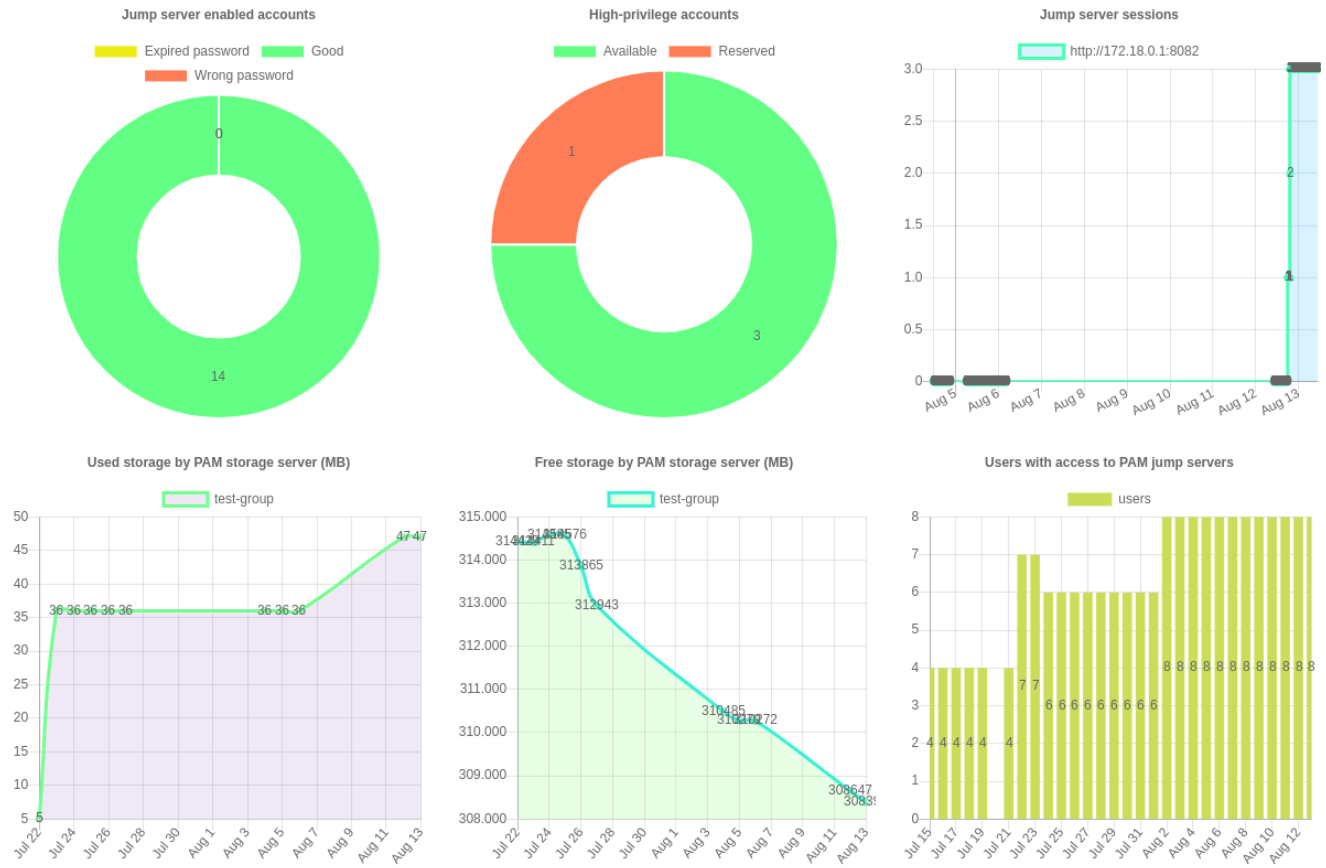
Description

> Soffid provides a monitoring functionality to consult all the information about the different Jump servers installed and configured.

The displayed info is the following:

- Jump server enabled accounts.
- High-privileged accounts.
- Jump server sessions.
- Used storage by PAM storage server.
- Free storage by PAM storage server.
- User with access to PAM jump servers.

Screen overview



Related objects

- Jump servers: Configure PAM session servers
- High-privileged accounts: Accounts

> To activate this view you will need to enable the **Feed statistic tables** task on the Scheduled tasks page.

Search in PAM recordings

Description

Soffid provides the functionality that allows searching for information about the PAM recording sessions.

That option is located on `Main Menu > Administration > Monitoring and reporting > Search in PAM recordings`

First of all, to query the PAM recording, you could apply some filters to refine your search. Then, when you click the Search button, Soffid will show you all the recording sessions that comply with the criteria specified.

If you click on one record, Soffid will show you a new page with all the data about the session and the recorded video. If you query with a typed keys filter, a bookmark with the minute and second will show, and it will allow you to go directly to that point and view the action.

Screen overview

https://www.youtube.com/embed/v1OR_1KMcTQ?rel=0

Standard attributes

- **Jum server group**: used to connect to the system.
- **URL:** service URL
- **Typed keys:** allows you to search in PAM recording
  - **Typed keys** by the user on the system.
    - Other information:
      - violation of rule
      - Ctrl
      - "[ctrl]+l"
      - "[ctrl]+d"
      - ...

    - **Screenshot contents** by screen content
- **User name:** user who created the session.
- **Start date**

Actions

Download CSV file	Allows you to download a CSV file with the PAM recording information.
Search	Allows you to query the PAM recording by applying some filters.
View recording	Allows you to view the recording. You need to click on the record of the PAM recording that you want to view, then Soffid will show you a new page with all the information about the session and the recording video.

Access logs

Description

The access log page allows querying all the information about the opened sessions.

Note that any session that was active during the specified date will be shown, even when it started before of finished after that date.

Screen overview

https://www.youtube.com/embed/rnTFtLeyi3k?rel=0

Custom attributes

- **Type**
- **Protocol**: access protocol.
  - SSO
  - SAML
  - PAM
  - CONSOLE
- **Start date**: date and time when start the access.
- **End date**: date and time when end the access.
- **Session**: session identifier.
- **Server**
- **Client**
- **User**: user who perform the access.
- **Information**: additional connection information.

- When the information is about the Authentication method, there are the following options:
  - **P**: Password
  - **K**: Kerberos
  - **E**: Broker
  - **O**: OTP
  - **M**: Email
  - **S**: SMS
  - **I**: PIN
  - **C**: Certificate
  - **F**: Finger print
  - **Z**: Push

Actions

Query	Allows you to query accounts through different search systems, Quick and Advanced.
Add or remove columns	Allows to show and hide columns in the table.
Download CSV file	Allows to download a CSV file with the information of access logs.

Sessions

Description

The sessions page displays the current open sessions made with ESSO, WSSO or PAM for which the user is the owner.

This functionality allows the owner users, with appropriate privileges, to open and view online a session opened by another user. It also allows them to interact if necessary.

Screen overview

https://www.youtube.com/embed/70uv0gVHEsQ?rel=0

Custom attributes

- **User**: name of the user who opened the session.
- **Device:** IP from which the connection was executed.
- **Client**
- **Type**:
  - ESSO
  - WSSO
  - PAM
- **Service URL:** connection URL
- **Account name**: user account name to connect.

Actions

Add or remove columns	Allows to show and hide columns in the table.
Download CSV file	Allows to download a CSV file with the information of access logs.

System Monitoring

Launcher

Soffid allows you to check the status of the launcher by browsing an URL:

Request

```
https://<your-host>/launch/status
```

For instance: http://demolab.soffid.pat.lab:8082/launch/status

Response

```
{
 "sessions":0,
 "status":"ok"
}
```

- **status** → “ok” the process is active.
- **sessions** → number of sessions the launcher is currently managing.

Store

In order to monitor the store, you will need the user and password with the appropriate permissions to view the status URL. This username and password come from the script executed to create the PAM containers.

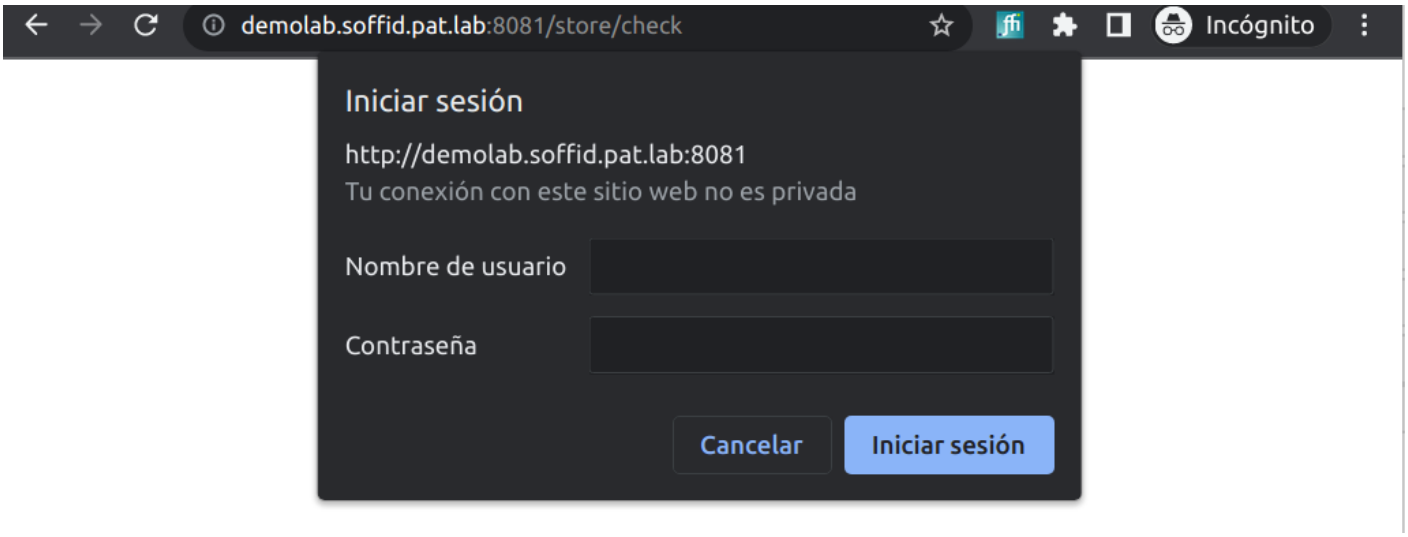
```
~/Downloads$ bash ./install-pam.sh
=====================
Creating store server
=====================
Waiting for store server
Creating launch server
============================================================
Process completed
Notice: You must register the store server in Soffid console:
User name: bubu-thinkpad
Password : DRFoeOsD02yph7DERNcAZB8jp3b67bO3D/Ax3uS4PbzuBnPbQLhR1lyAu9PFqRJ0
~/Downloads$ docker ps
CONTAINER ID IMAGE                 COMMAND                  CREATED         STATUS         PORTS
854d7aff5c0a soffid/pam-launcher   "/bin/sh -c /opt/sof…"   4 minutes ago   Up 4 minutes   0.0.0.0:8082->80
7d66a3d3cfa1 soffid/pam-store      "/bin/sh -c /opt/sof…"   4 minutes ago   Up 4 minutes   0.0.0.0:8081->80
```

To monitor the store you need to browse the following URL:

Request

```
https://<your-host>/store/check
```

For instance: http://demolab.soffid.pat.lab:8081/store/check



Response

```
{
  "usedSpace": 156933901,
  "freeSpace": 161442168832,
  "status": "OK"
}
```

- **status** → “OK” the process is active.
- **usedSpace** → occupied bytes.
- **freeSpace** → free bytes.