Preparation for installation

Active Directory

Indeed Identity PAM interacts with end users through an account that will read directory users and their attributes.

Account to use with user directory

1. Run the **Active Directory Users and Computers** snap-in
2. Open the context menu of organizational unit or container
3. Select **Create** - **User** item from the menu
4. Specify the user name, say, **IPAMManager**
5. Fill in the mandatory fields and complete the account creation

Alternatively, you can use an existing account.

Account for service operations in Active Directory

1. Start the **Active Directory Users and Computers** snap-in
2. Open the context menu of the Container or Organization Unit
3. Select **Create** - **User** item
4. Enter the name, for example, **IPAMADServiceOps**
5. Fill in the required fields and complete the creation of the account
6. Open the context menu of the container, organizational unit, or domain root and select the **Properties** item
7. Go to the **Security** tab
8. Click **Add**
9. Select **IPAMADServiceOps** account and click **Ok**
10. Click **Advanced**
11. Select **IPAMADServiceOps** and click **Edit**
12. For the field **Applies to:** set value **Descendant User objects**
13. In the **Permissions:** section check **Reset password**
14. Save all changes

Alternatively, you can use an existing account.

Storage of media files and shadow copies

File storages are necessary for aggregation and long-term storage of videos, screenshots and files transferred in sessions.

File storage account

A domain account is required to work with file storage, recommended to use the already created **IPAMStorageOps** account.

Create and configure file storage

1. Log in to the server, which will act as a file storage
2. reate folders, for example **MediaData**, **ShadowCopy**, **Screencasts**
3. Right click on the folder you created, select the item **Share with** > **Specific people**
4. Enter the username, for example **IPAMStorageOps** and click **Add**
5. In the "Permission level" column, click the **Read** value next to the **IPAMStorageOps** user and select **Read/Write** from the menu.
6. Finish by clicking **Share**

Data storage

Indeed Identity PAM uses Microsoft SQL Server or PostgreSQL Pro to store data. The following components require databases:

- **IPAMCore** - PAM Core component database is used to store Indeed Identity PAM privileged accounts, resources, permissions, and other service data

- **IPAMJobs** - PAM Core component database is used to store scheduled jobs
- **IPAMIdp** - IdP component database is used to store authenticators of Indeed Identity PAM users and administrators
- **ILS** - Log Server component database is used to store the Indeed Identity PAM event

Database creation

1. Run **Microsoft SQL Management Studio** (SSMS) and connect to Microsoft SQL Server instance
2. Open the context menu of **Databases** item
3. Select the **New Database** item
4. Specify a database name, for example **IPAMCore**, **IPAMJobs**, **IPAMIdP**, **ILS**
5. Click **OK**

1. Launch **pgAdmin** and connect to the PostgreSQL Pro server
2. Open the context menu of the **Databases** item
3. Select **Create**, **Database**
4. Specify a database name, for example: **IPAMCore**, **IPAMJobs**, **IPAMIdP**, **ILS**
5. Click **Save**

Creating a service account to work with data storage

1. Start **Microsoft SQL Management Studio** (SSMS) and connect to the Microsoft SQL Server instance
2. Expand the **Security** item
3. Open the context menu of **Logins** item
4. Select the **Create login** item
5. Enter the name, for example **IPAMSQLServiceOps**
6. Select **SQL Server authentication** item and fill in the required fields
7. Switch to **User Mapping** item
8. Check **IPAMCore**, **IPAMTasks**, **IPAMIdP** and **ILS** databases
9. Check database roles **db_owner**, **db_datareader** and **db_datawriter**
10. Click **OK**

1. Launch **pgAdmin** and connect to the PostgreSQL Pro server
2. Open the context menu of the **Login/Group Roles** item
3. Select **Create**, **Login/Group Role**
4. Specify a **Name**, for example **IPAMSQLServiceOps**
5. Go to **Definition** tab, enter the new password for account
6. Go to **Privileges** tab, check **Yes** for **Can Login?** and **Superuser?** items
7. Click **Save**, repeat for the rest of the databases.

The grants **db_owner** for Microsoft SQL Server and **Superuser** for PostgreSQL are required only for the first access to the database.