Practical No. - 6

Aim: To study and implementation of identity management.

Theory:

Identity Management, often referred to as Identity and Access Management (IAM), is a framework of policies and technologies ensuring that the right individuals have access to the technology resources they need in an organization. It plays a crucial role in any organization's security and operational efficiency. Here are the core components and concepts involved in Identity Management:

1. **Identification**: This involves recognizing a user in a system. It can be through a username, emailaddress, or any unique identifier.

2. **Authentication**: Once a user is identified, the system needs to verify their identity. This is typicallydone through passwords, biometric verification, tokens, or other forms of credentials.

3. **Authorization**: After authentication, the system determines what resources the user can access and what operations they can perform. This is governed by policies and rules set up by the organization.

4. **User Management**: It involves creating, updating, disabling, and deleting user accounts and profilesas well as managing their access rights.

5. **Role-Based Access Control (RBAC)**: In RBAC, access rights are grouped by role name, and access to resources is restricted to users based on their roles. This simplifies the management of user permissions.

6. **Attribute-Based Access Control (ABAC)**: This model controls access based on attributes (characteristics) of users, resources, and the environment, offering more granular access control thanRBAC.

7. **Single Sign-On (SSO)**: SSO allows users to log in once and gain access to multiple systems withoutbeing prompted to log in again at each of them.
8. **Multi-Factor Authentication (MFA)**: MFA enhances security by requiring two or more verification factors to gain access to a resource, such as something you know (password), something you have (security token), or something you are (biometric verification).

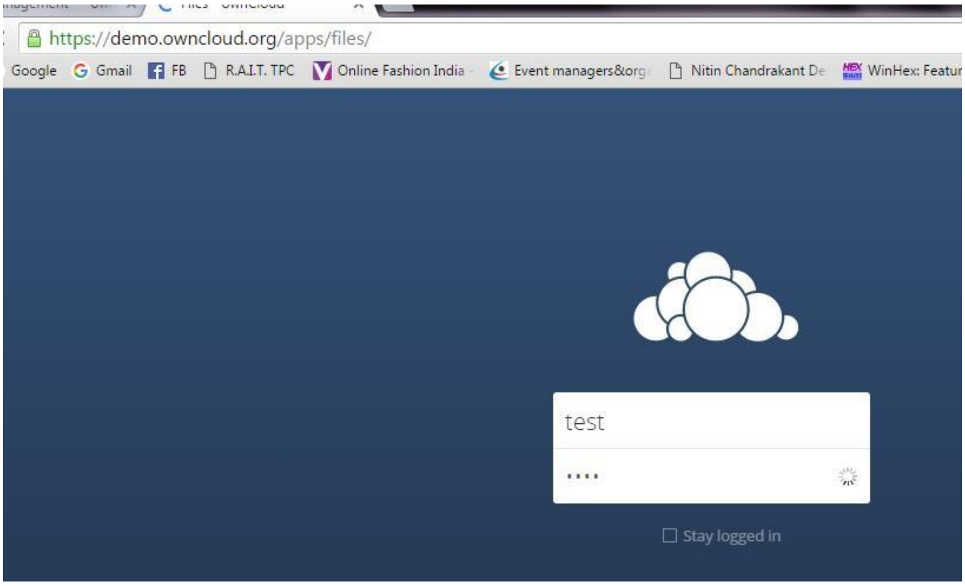
9. **Provisioning and De-provisioning**: Provisioning involves granting users access to resources they need, while de-provisioning involves removing access when it is no longer needed or when the userleaves the organization.

10. **Compliance Management**: Ensures that the organization's identity management practices complywith legal and regulatory requirements.

Identity Management solutions often leverage advanced technologies like artificial intelligence and machine learning to automate processes, detect anomalies, and enhance security. Effective Identity Management helps organizations minimize the risk of unauthorized access, improve user productivity by streamlining access processes, and reduce the costs associated with managing user identities and permissions.

Procedure:

Step 1 Go to demo.owncloud.org.



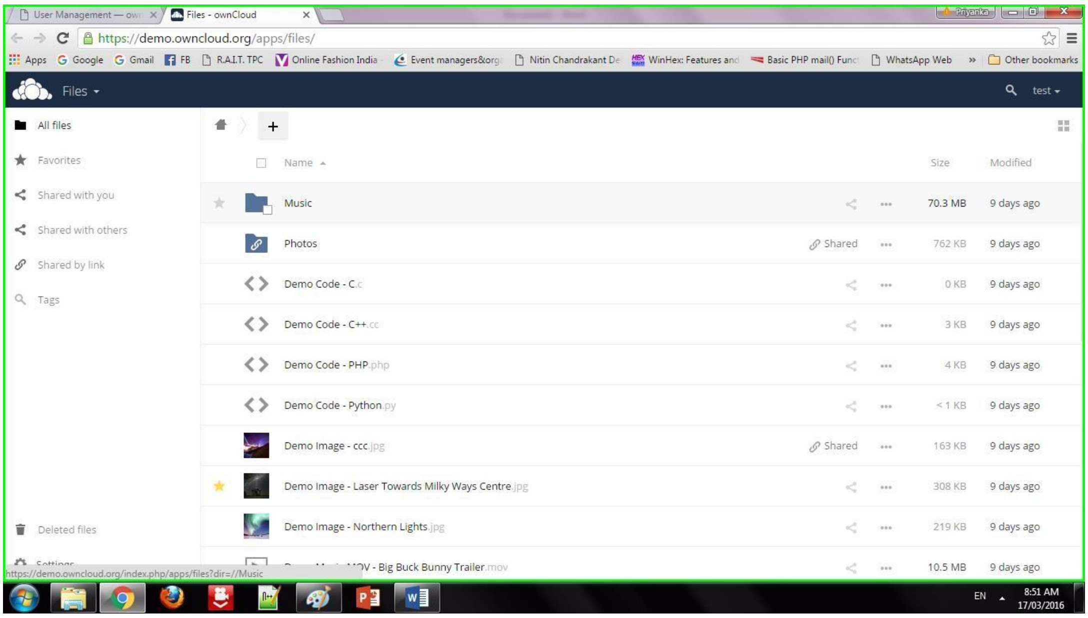
https://demo.owncloud.org/apps/files/

test

••••

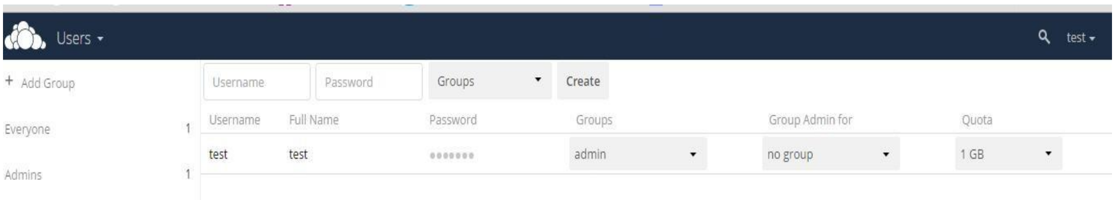
□ Stay logged in

Step 2 : By default, the ownCloud Web interface opens to your Files page. You can add, remove, and share files, and make changes based on the access privileges set by you (if you are administering the server) or by your server administrator. You can access your ownCloud files with the ownCloud web interface and create,preview, edit, delete, share, and re-share files. Your ownCloud administrator has the option to disable these features, so if any of them are missing on your system ask your server administrator

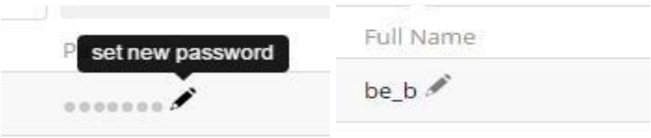


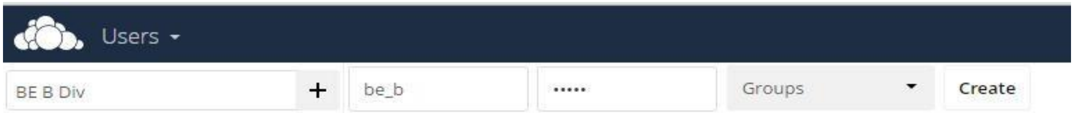
Name		Size	Modified
Music		70.3 MB	9 days ago
Photos	Shared	762 KB	9 days ago
Demo Code - C.c		0 KB	9 days ago
Demo Code - C++.cc		3 KB	9 days ago
Demo Code - PHP.php		4 KB	9 days ago
Demo Code - Python.py		< 1 KB	9 days ago
Demo Image - ccc.jpg	Shared	163 KB	9 days ago
Demo Image - Laser Towards Milky Ways Centre.jpg		308 KB	9 days ago
Demo Image - Northern Lights.jpg		219 KB	9 days ago
Demo Movie - MOV - Big Buck Bunny Trailer.mov		10.5 MB	9 days ago

Step 3: **Apps Selection Menu:** Located in the upper left corner, click the arrow to open a dropdown menu to navigate to your various available apps. **Apps Information field:** Located in the left sidebar, this provides filters and tasks associated with your selected app. **Application View:** The main central field in the ownCloud user interface. This field displays the contents or user features of your selected app.

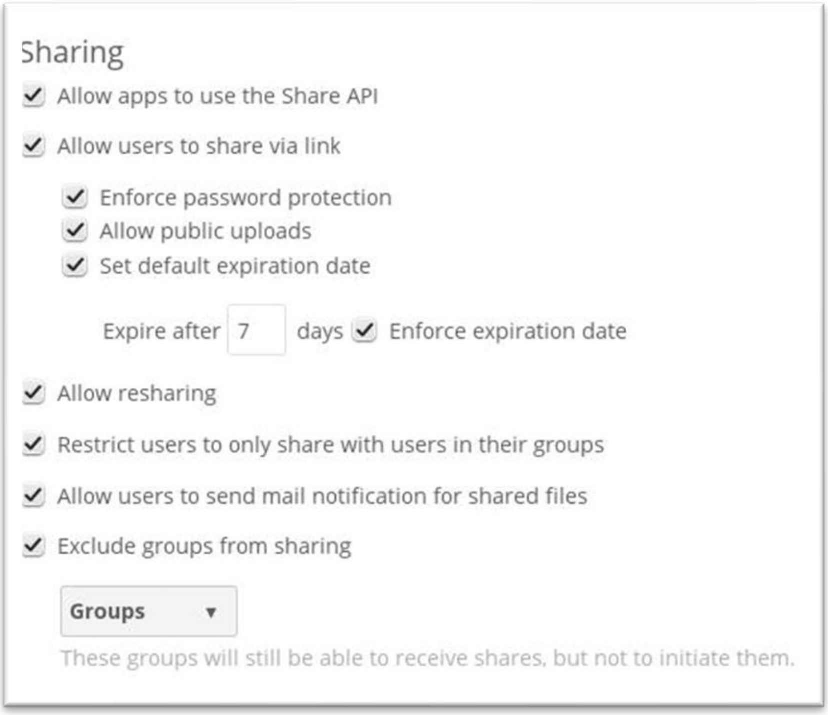


Username	Full Name	Password	Groups	Group Admin for	Quota
test	test	•••••••	admin	no group	1 GB





Step 4: Share the file or folder with a group or other users, and create public shares with hyperlinks. You can also see who you have shared with already, and revoke shares by clicking the trash can icon. If username auto-completion is enabled, when you start typing the user or group name ownCloud will automatically complete it for you. If your administrator has enabled email notifications, you can send an email notification of the new share from the sharing screen.



Sharing

☑ Allow apps to use the Share API

☑ Allow users to share via link

- ☑ Enforce password protection
- ☑ Allow public uploads
- ☑ Set default expiration date

Expire after 7 days ☑ Enforce expiration date

☑ Allow resharing

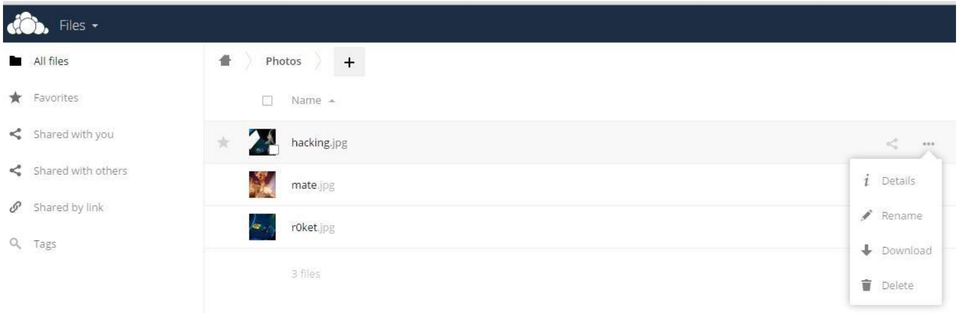
☑ Restrict users to only share with users in their groups

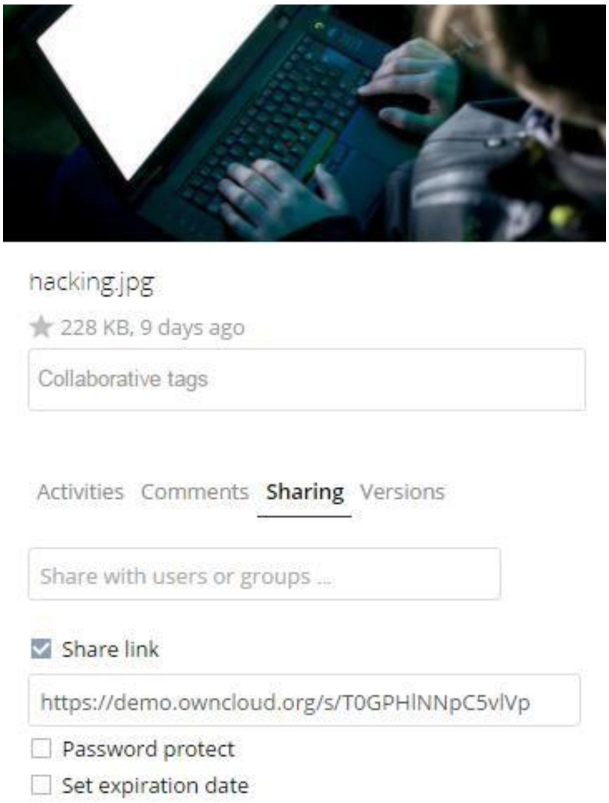
☑ Allow users to send mail notification for shared files

☑ Exclude groups from sharing

Groups ▾

These groups will still be able to receive shares, but not to initiate them.





hacking.jpg

★ 228 KB, 9 days ago

Collaborative tags

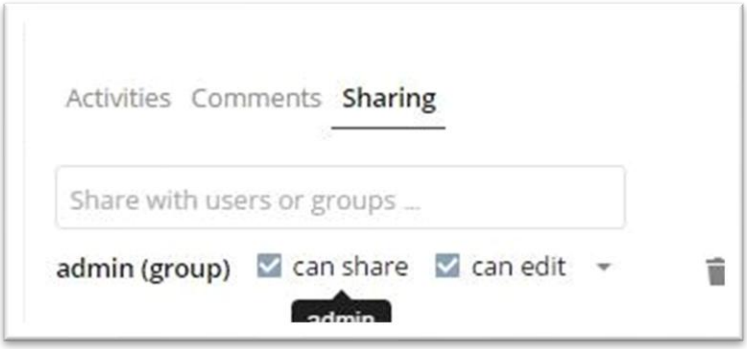
Share with users or groups ...

☑ Share link

https://demo.owncloud.org/s/T0GPHlNNpC5vlVp

□ Password protect

□ Set expiration date



admin (group) ☑ can share ☑ can edit

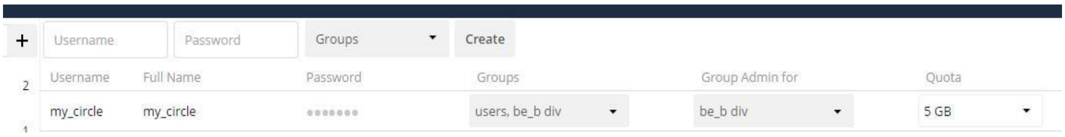
Step 5: Five Share permissions are :

Can share; allows the users you share with to re-share.

Can edit; allows the users you share with to edit your shared files, and to collaborate using the Documentsapp.

Create; allows the users you share with to create new files and add them to the share.

Change; allows uploading a new version of a shared file and replacing it.
Delete; allows the users you share with to delete shared files.



Username	Full Name	Password	Groups	Group Admin for	Quota
my_circle	my_circle	•••••••	users, be_b div	be_b div	5 GB

Conclusion:

We have studied how to use ownCloud for ensuring identity management of the users. We can create multiple groups and provide privileges to view or modify data as per defined permissions. It also enables simplified look and feel to be used by anyone.