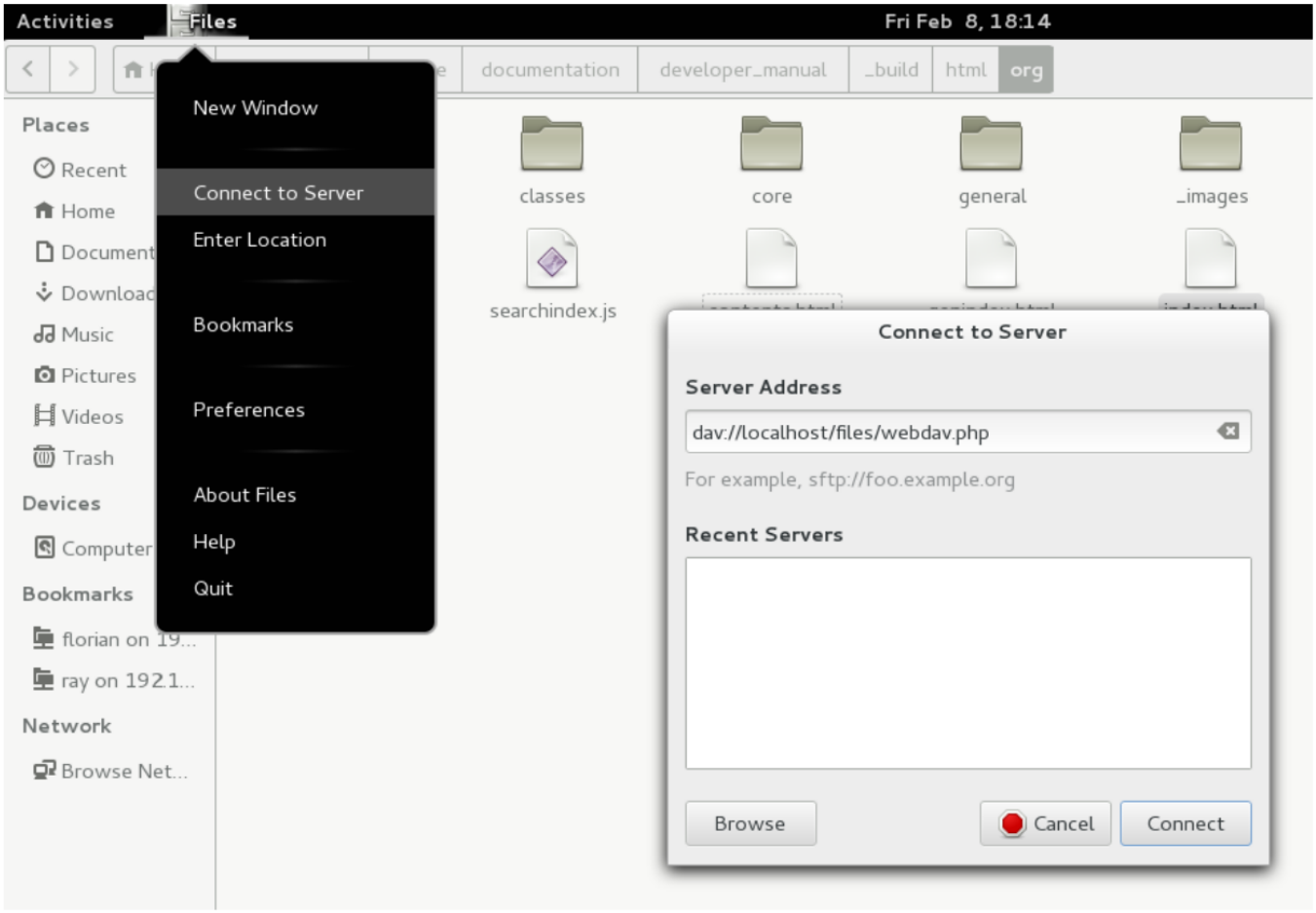
Advanced Customization

- Accessing Nextcloud files using WebDAV
- Desktop Synchronization Client
- Encryption

Accessing Nextcloud files using WebDAV

Nextcloud supports the WebDAV protocol, and you can connect and synchronize with your Nextcloud files over WebDAV. There are official desktop and mobile applications available. For the Nextcloud documentation, check out the official documentation

Linux (Gnome):



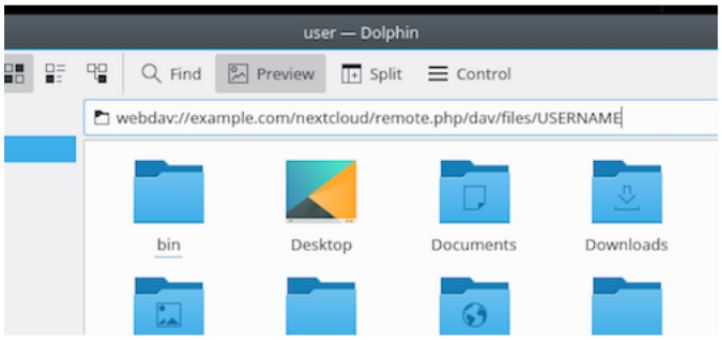
If you configure your Nextcloud account in the GNOME Control Center , your files will automatically be mounted by Nautilus as a WebDAV share.

Linux (KDE):

Accessing files with KDE and Dolphin file manager

To access your Nextcloud files using the Dolphin file manager in KDE, use the `webdav://` protocol:

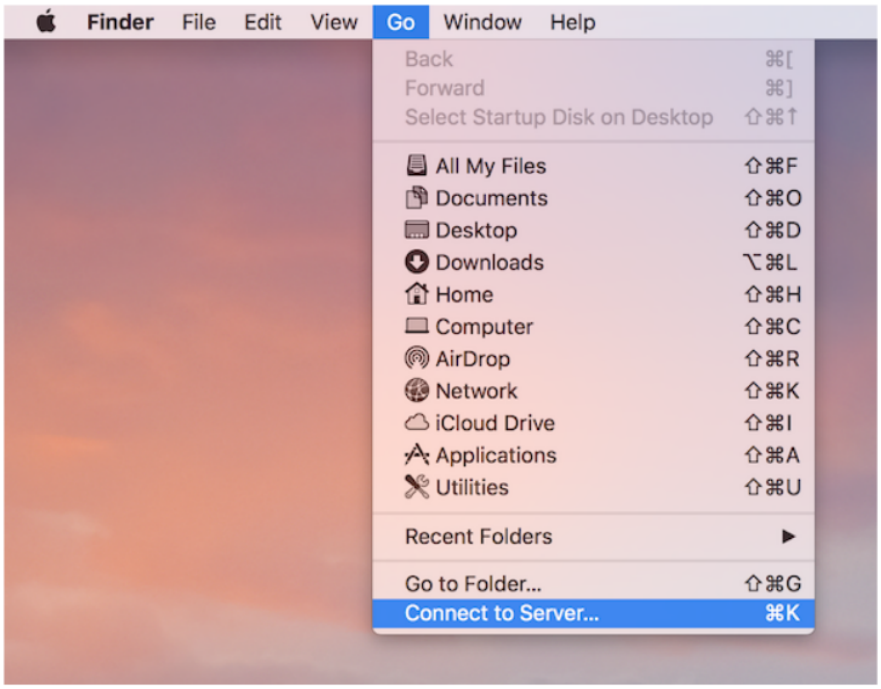
```
webdav://example.com/nextcloud/remote.php/dav/files/USERNAME/
```



Mac:

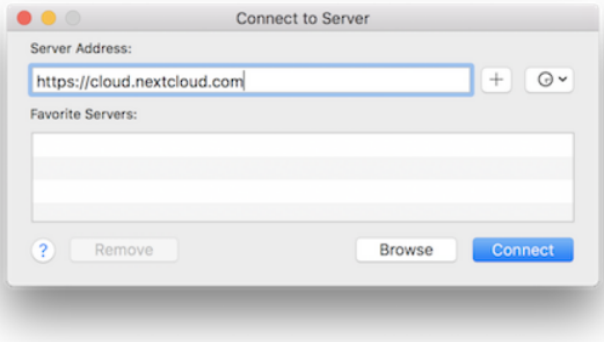
To access files through the macOS Finder:

1. From the Finder's top menu bar, choose **Go > Connect to Server…**



2. When the **Connect to Server…** window opens, enter your Nextcloud server's WebDAV address in the **Server Address:** field, ie:

   https://cloud.YOURDOMAIN.com/remote.php/dav/files/USERNAME/



3. Click **Connect**. Your WebDAV server should appear on the Desktop as a shared disk drive.

Curl:

4.2.11 Accessing files using cURL

Since WebDAV is an extension of HTTP cURL can be used to script file operations.

To create a folder with the current date as name:

```
$ curl -u user:pass -X MKCOL "https://example.com/nextcloud/remote.php/dav/files/
↪USERNAME/$(date '+%d-%b-%Y')"
```

To upload a file `error.log` into that directory:


```
$ curl -u user:pass -T error.log "https://example.com/nextcloud/remote.php/dav/files/
↪USERNAME/$(date '+%d-%b-%Y')/error.log"
```

To move a file:

```
$ curl -u user:pass -X MOVE --header 'Destination: https://example.com/nextcloud/
↪remote.php/dav/files/USERNAME/target.jpg' https://example.com/nextcloud/remote.php/
↪dav/files/USERNAME/source.jpg
```

To get the properties of files in the root folder:

```
    $ curl -X PROPFIND -H "Depth: 1" -u user:pass https://example.com/nextcloud/
↪remote.php/dav/files/USERNAME/ | xml_pp
    <?xml version="1.0" encoding="utf-8"?>
<d:multistatus xmlns:d="DAV:" xmlns:oc="http://nextcloud.org/ns" xmlns:s="http://
↪sabredav.org/ns">
  <d:response>
    <d:href>/nextcloud/remote.php/dav/files/USERNAME/</d:href>
    <d:propstat>
      <d:prop>
        <d:getlastmodified>Tue, 13 Oct 2015 17:07:45 GMT</d:getlastmodified>
        <d:resourcetype>
          <d:collection/>
        </d:resourcetype>
        <d:quota-used-bytes>163</d:quota-used-bytes>
        <d:quota-available-bytes>11802275840</d:quota-available-bytes>
        <d:getetag>"561d3a6139d05"</d:getetag>
      </d:prop>
      <d:status>HTTP/1.1 200 OK</d:status>
    </d:propstat>
  </d:response>
  <d:response>
    <d:href>/nextcloud/remote.php/dav/files/USERNAME/welcome.txt</d:href>
    <d:propstat>
      <d:prop>
        <d:getlastmodified>Tue, 13 Oct 2015 17:07:35 GMT</d:getlastmodified>
        <d:getcontentlength>163</d:getcontentlength>
        <d:resourcetype/>
        <d:getetag>"47465fae667b2d0fee154f5e17d1f0f1"</d:getetag>
        <d:getcontenttype>text/plain</d:getcontenttype>
      </d:prop>
      <d:status>HTTP/1.1 200 OK</d:status>
    </d:propstat>
  </d:response>
```

Desktop Synchronization Client

The Nextcloud Desktop Sync client allows you to:

- Specify one or more directories on your computer that you want to synchronize to the Nextcloud server.
- Always have the latest files synchronized, wherever they are located.

Files are always automatically snychronized between the Nextcloud server and local PC.

Check out the documentation from the upstream project for more information and how to install.

Encryption

Encryption is one of the steps to take when designing a system with Defence in depth. Here we go over what you need to be concerned about and different implementations to consider.

Threat Model

Threat modelling is hard. The most widely-applicable framework that I have stumbled across is to frame up your model with respect to the following scopes, from lowest to highest:

- Neighborhood Hacker
- Corporate Surveillance
- Nation-State Espionage

Consider at which level you would like to defend against when considering the options available to you.

Responsibility Levels

There are three levels of responsibility for any hosted service:

- Physical/Infrastructure
- Service Provider/OS Admin
- Application admin/consumer

Physical/Infrastructure

Digital Ocean:

- Local Droplet Storage: https://www.digitalocean.com/community/questions/droplet-native-storage-is-it-encrypted-similarly-to-block-storage-volumes?answer=54705
- Block Storage: https://docs.digitalocean.com/products/volumes/

Service Provider/OS Admin

- Enabled:
  - HTTPS: https://blog.securityevaluators.com/does-https-protect-your-privacy-9e8903f576d3
- Planned:
  - LUKS: https://en.wikipedia.org/wiki/Linux_Unified_Key_Setup
  - Encrypted Tarballs: https://www.tecmint.com/encrypt-decrypt-files-tar-openssl-linux/

Application Admin/Consumer

Built-In Nextcloud Functionality: https://nextcloud.com/blog/encryption-in-nextcloud/

- Server-Side Storage Encryption:
  - https://nextcloud.com/encryption/
  - https://docs.nextcloud.com/server/latest/user_manual/en/files/encrypting_files.html
  - A note on local storage:
    A server-wide key stores a server password in the Nextcloud data directory and uses it to decrypt the server key in the users' data directory, which in turn is used to decrypt data.

    When using per-user keys, the key in the data directory is per user and encrypted with the user password. We take great care to ensure keys never enter storage but keys will be kept in memory on the Nextcloud server for the duration of user login sessions to facilitate decryption and encryption of data.

    Per-user keys only offer additional protection over a server-wide key in the case of physical theft of the Nextcloud server and storage or a security breach of the sever *provided the user(s) do NOT log in for the duration of the breach*.
- End-to-End File-level Encryption:
  - https://nextcloud.com/endtoend/
  - https://github.com/nextcloud/end_to_end_encryption
  - https://www.techrepublic.com/article/how-to-enable-end-to-end-encryption-for-the-nextcloud-app/