

Palvelut ja SSH-tunnelit

Luento 4

Niklas Halonen, Joonas von Lerber

2025-04-23

Otaniemen lukio

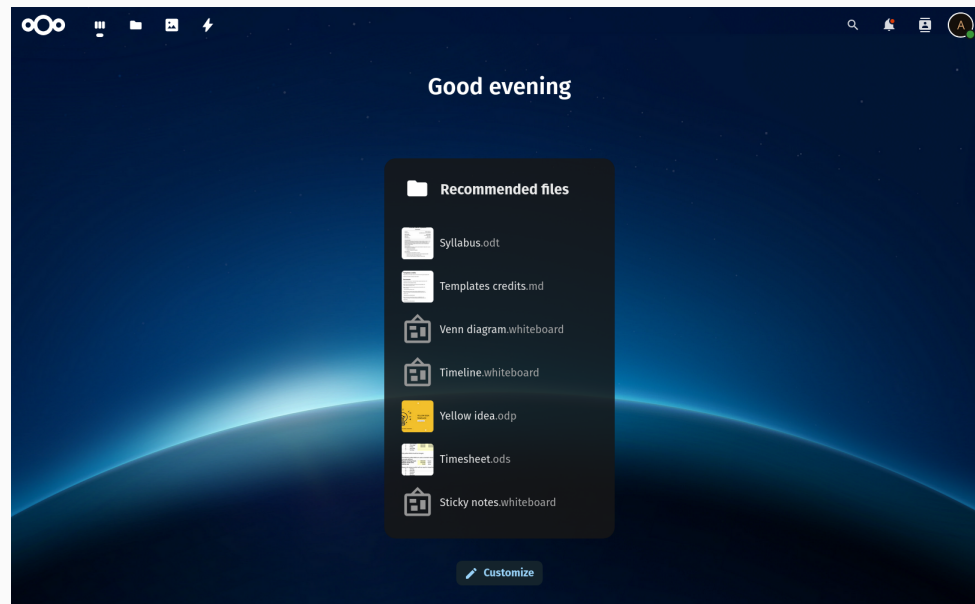
1. Nextcloud-palvelun asentaminen Ubuntu-serverille
2. SSH-tunnelin muodostaminen
3. Systemd-palvelut
4. Nextcloud-palvelimen konfigurointi

Nextcloud

Nextcloud on henkilökohtaisen tiedon, dokumenttien, kalenterien yms hallintajärjestelmä.

Se on avointa lähdekoodia¹ (AGPL-lisenssillä) joka tarkoittaa että sen voi asentaa omalle palvelimelle ilmaiseksi.

Tällä tunnilla asennamme Nextcloudin koska se on helppoa.



Nextcloud dashboard

¹Lähdekoodi

			
Licensing	Open source	Proprietary	Proprietary
Unlimited storage and amount of files	✓	✓	✓
Large file support	✓	✓	10GB
Self hosted / on premises	✓	✗	✗

Nextcloudin (tai muun palvelun) ylläpito

- ⚠ Vaikka Nextcloud (tai muu palvelu) on helppo asentaa, se ei tarkoita, että sen ylläpito on helppoa!
- ⚠ Jos Nextcloud-instanssi (tai muu palvelu) on julkiverkossa, niin sitä on päivitettävä säännöllisesti!

Palomuurit ja avoimet portit (tärkeää!)

- Fablabin tarjoama palvelininfrastruktuuri mahdollistaa jokaisen virtuaalipalvelimen HTTP-porttiin (80) pääsyn julkiverkosta.
- Käytännössä järjestelmä toimii palomuurina siten että vain HTTP-porttiin voi saada yhteyden ilman esim. SSH-pääsyjä self-hosted palvelimelle.
- Tietoturvallisuuden kannalta on kriittistä, että portissa 80 kuunteleva ohjelmisto (esim. Nextcloud) ei ole haavoittuvainen hyökkäyksillä.
- Kun pyörität tulevaisuudessa omaa palvelinta, varmista että yksityinen tieto on suojassa.
 - Tämän varmistamiseksi kannattaa olla VPN-yhteys tai muu salattu yhteys palveluihin jotka käsittelevät yksityistä tietoa.
 - Kotireitittimen NAT-tauluun ei tule avata (forward) porttia, ellei ole aivan varma että osaa tehdä sen turvallisesti.

How To Install and Configure Nextcloud on Ubuntu 22.04 ([digitalocean.com](https://www.digitalocean.com/articles/how-to-install-and-configure-nextcloud-on-ubuntu-22-04))

– löytyy valitsemallasi hakukoneella hakemalla “nextcloud digitalocean ubuntu”.

Edetään yhdessä **Step 3 – Adjusting the Trusted Domains** asti.

Nämä palvelut asentuvat samalla¹ kun asennat Nextcloudin:

1. Apache: HTTP-palvelin
2. MySQL: SQL-tietokanta
3. Redis: avain-arvo-tietokanta
4. Logrotate: pitkäaikaisten lokien hallinta
5. Cron: ajoittain taustalla tapahtuvat “jobit”

¹Moderneissa Ubuntuissa snap-työkalu asentaa

SSH-tunneli ja portinohjaus

`ssh`:lla voi ohjata että joku portti omalta koneelta ohjataan suoraan toiseen porttiin toisella koneella. Tähän käytetään `-L SRCPORT:DSTHOST:DSTPORT` asetusta. Portinohjaus on aktiivinen kunnes SSH-yhteys katkaistaan.

Näin paikallinen (oppilaskoneen) portti 8080 ohjataan pannun porttiin 80.

```
ssh nimi@pannu [-J ...] -L 8080:localhost:80
```

Nyt, jos pannulla portissa 80 pyörii esim. nginx, voi siihen yhdistää avaamalla selaimella osoitteen <https://localhost:8080>.

Portinohjaus toiseen verkkoon

SSH:n avulla voi myös yhdistää toisessa verkossa olevaan palvelimeen asettamalla **DSTHOST** muuhun kuin **localhost**:

```
ssh nimi@pannu [-J ...] -L 3000:google.com:80
```

Tässä tilanteessa ohjaamme portin 3000 yhdistämään **google.com** portiin 80. Kun selaimella avaa osoitteen <https://localhost:3000> niin yhteys Googlen palvelimelle muodostuu. Huom: Google haluaa käyttää salattua HTTPS-yhteyttä, joten verkkosivu ei toimi tavalliseen tapaan vaan antaa 404 virheen.

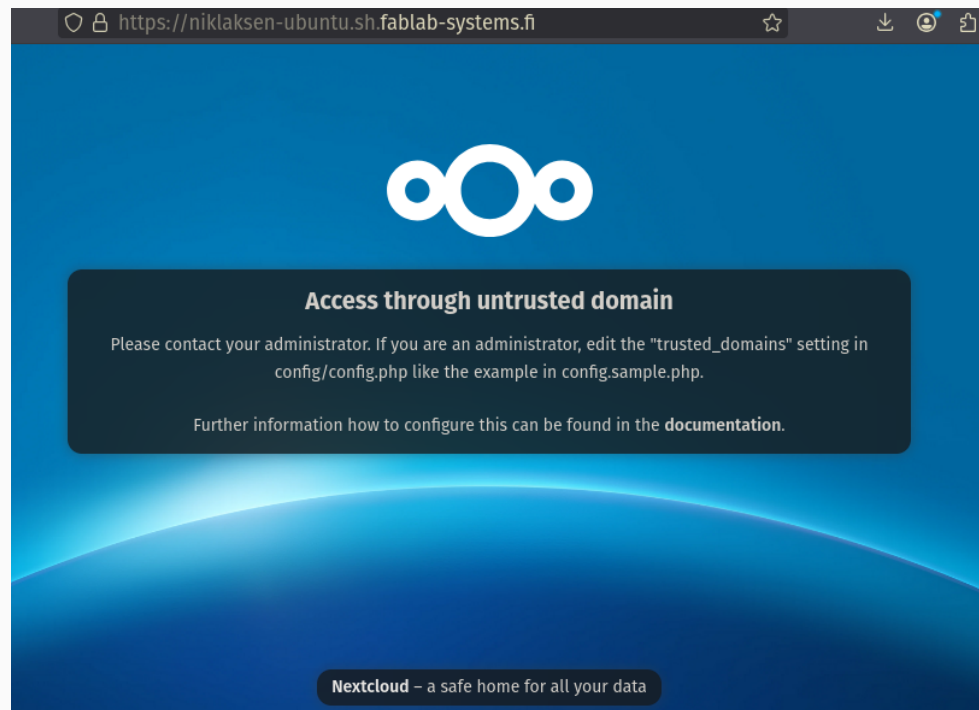
<https://www.linux.fi/wiki/SSH#Tunneli>

Portinohjaus ja palomuuuri

- Nextcloud oletuksena estää yhdistämisen julkisen verkon kautta, mutta paikallinen (**localhost**) yhteys on sallittu.
- Voimme käyttää SSH:n portinohjausta yhdistämään Nextcloudiin ihan kuin yhteys olisi paikallinen:

```
ssh nimi@pannu [-J ...] -L  
8080:localhost:80
```

- Portinohjausta voidaan yleisestikin käyttää ohittamaan palomuurien asettamia rajoitteita.



Kuvassa Nextcloud ilmoittaa että yhteys ei ole sallittu ulkopuolelta.

Yleisimpiin ylläpitotoimiin kuuluu:

1. Ohjelmiston päivittäminen säännöllisesti
2. Lokien seuraaminen ja virheisiin reagoiminen

Nextcloudin lokit löytyvät seuraavasta hakemistosta, josta esim. `apache_access.log` kertoo palveluun muodostetuista yhteyksistä:

```
sudo tail -f /var/snap/nextcloud/current/logs/apache_access.log
```

Esim. tiedosto `mysql_errors.log` kuulostaa viittaavan mahdollisiin virheisiin (error) joita MySQL-palvelu on tuottanut, mutta kyseessä onkin vain tavalliset lokit eikä virhetapahtumat...

Nextcloudin konfigurointi

- occ (OwnCloud Console), `nextcloud.occ`

```
niklash@niklaksen-ubuntu ~> sudo nextcloud.occ status
```

```
- installed: true
- version: 31.0.2.1
- versionstring: 31.0.2
- edition:
- maintenance: false
- needsDbUpgrade: false
- productname: Nextcloud
- extendedSupport: false
```

- Ylläpitäjän manuaali: https://docs.nextcloud.com/server/latest/admin_manual/

Jotain huomioita löytyy Nextcloudin admin overview:stä:

Security & setup warnings ⓘ

It's important for the security and performance of your instance that everything is configured correctly. To help you with that we are doing some automatic checks. Please see the linked documentation for more information.

✖ There are some errors regarding your setup.

- The reverse proxy header configuration is incorrect. This is a security issue and can allow an attacker to spoof their IP address as visible to the Nextcloud. For more details see the [documentation ↗](#).
- Accessing site insecurely via HTTP. You are strongly advised to set up your server to require HTTPS instead. Without it some important web functionality like "copy to clipboard" or "service workers" will not work! For more details see the [documentation ↗](#).
- 1 error in the logs since April 15, 2025, 9:46:27 PM
- Some headers are not set correctly on your instance - The 'Strict-Transport-Security' HTTP header is not set (should be at least `15552000` seconds). For enhanced security, it is recommended to enable HSTS. For more details see the [documentation ↗](#).
- Your installation has no default phone region set. This is required to validate phone numbers in the profile settings without a country code. To allow numbers without a country code, please add "default_phone_region" with the respective ISO 3166-1 code of the region to your config file. For more details see the [documentation ↗](#).
- You have not set or verified your email server configuration, yet. Please head over to the "Basic settings" in order to set them. Afterwards, use the "Send email" button below the form to verify your settings. For more details see the [documentation ↗](#).
- The PHP module "imagick" is not enabled although the theming app is. For favicon generation to work correctly, you need to install and enable this module. For more details see the [documentation ↗](#).

Please double check the [installation guides ↗](#), and check for any errors or warnings in the [log](#).

Check the security of your Nextcloud over [our security scan ↗](#).

Version

Nextcloud Hub 10 (31.0.2)