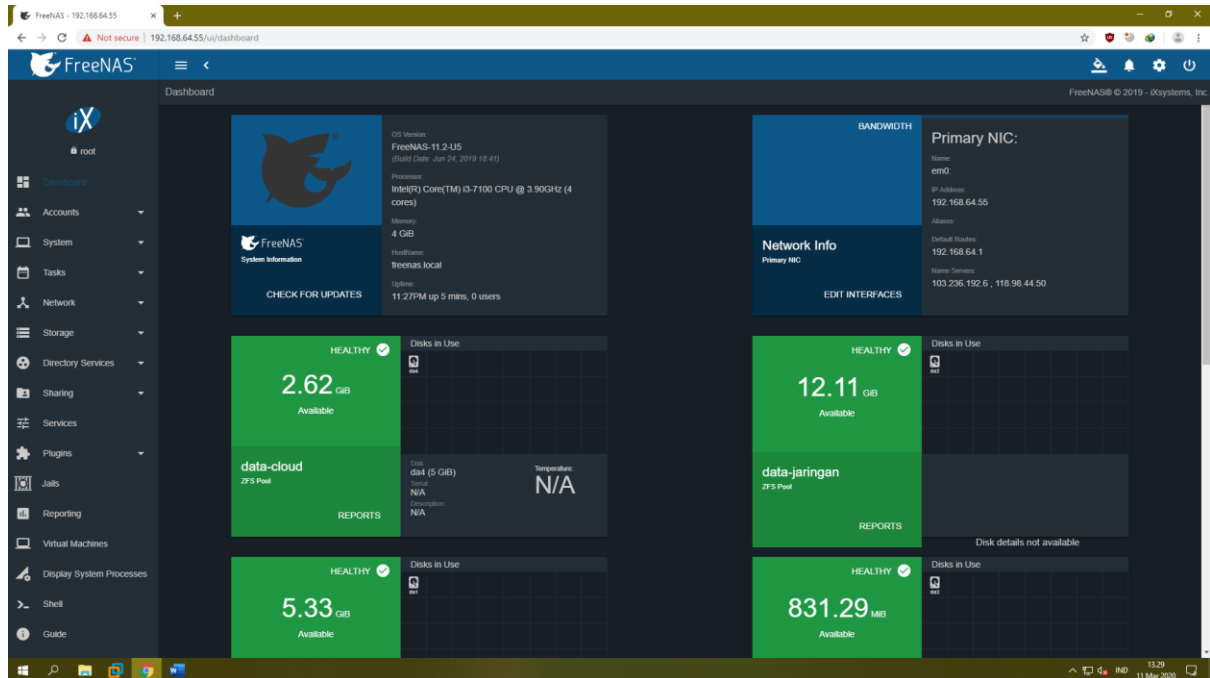


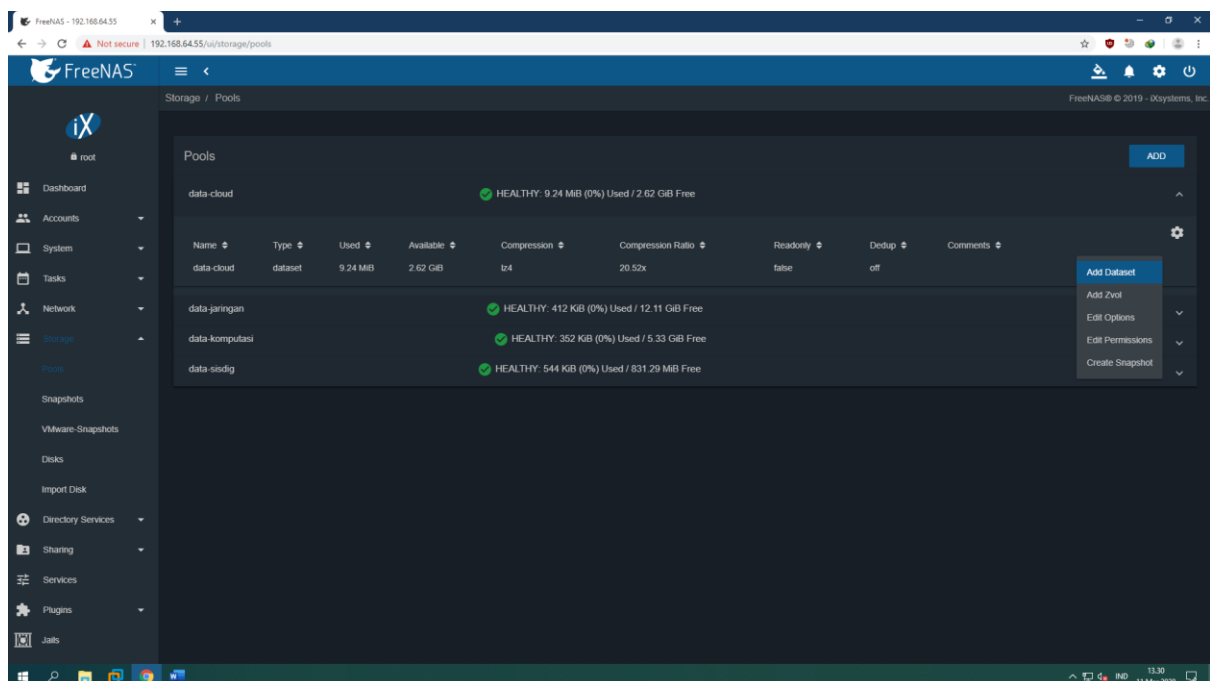
Sakti Wicaksono / 123170031 / E

## Konfigurasi S3 Bucket Service

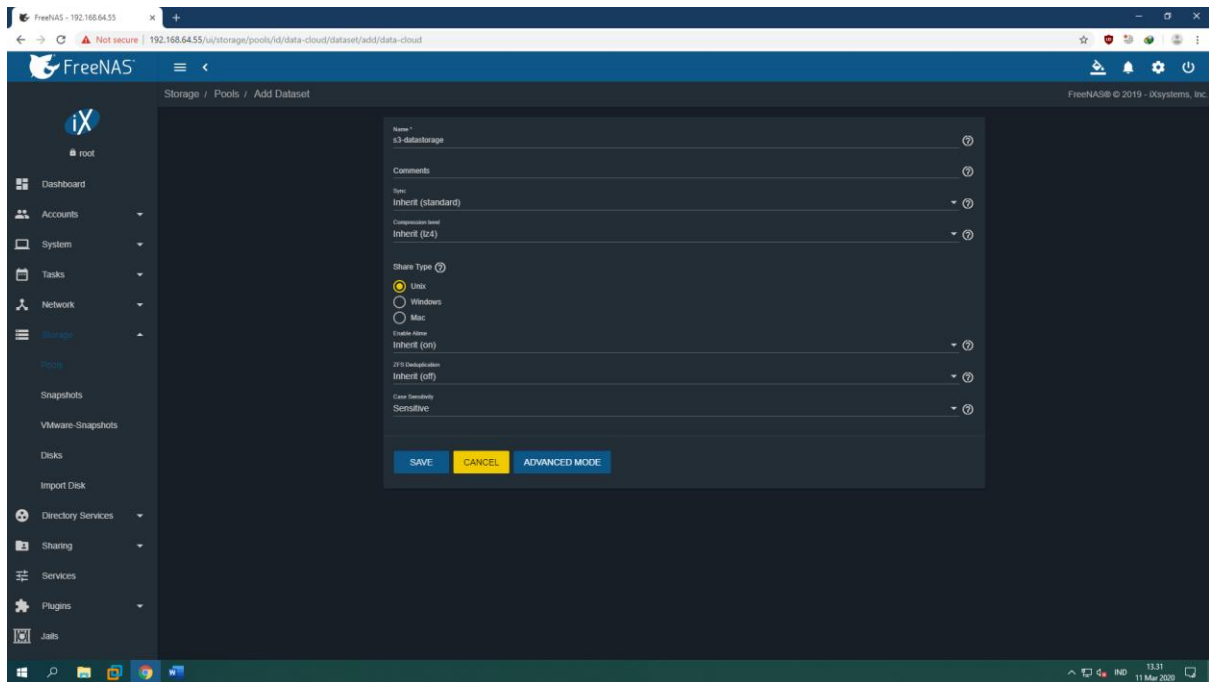
### 1. Login Dashboard FreeNAS



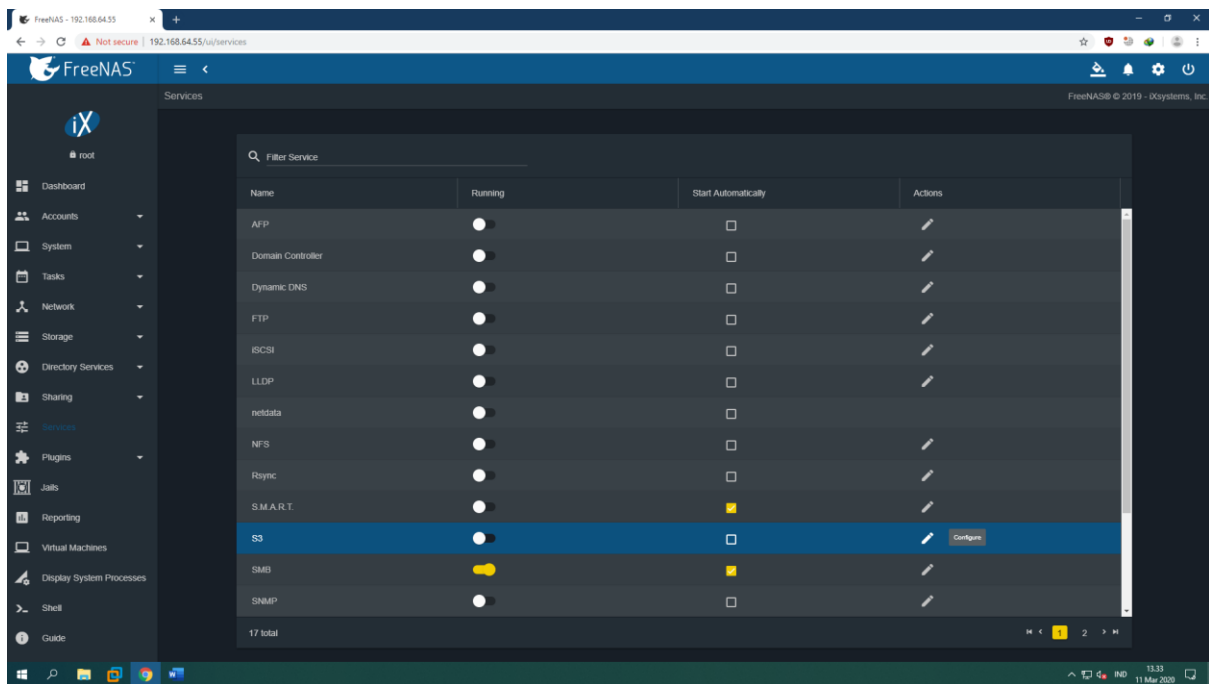
### 2. Masuk Menu Storage Pool, pada pool pilih Add Dataset



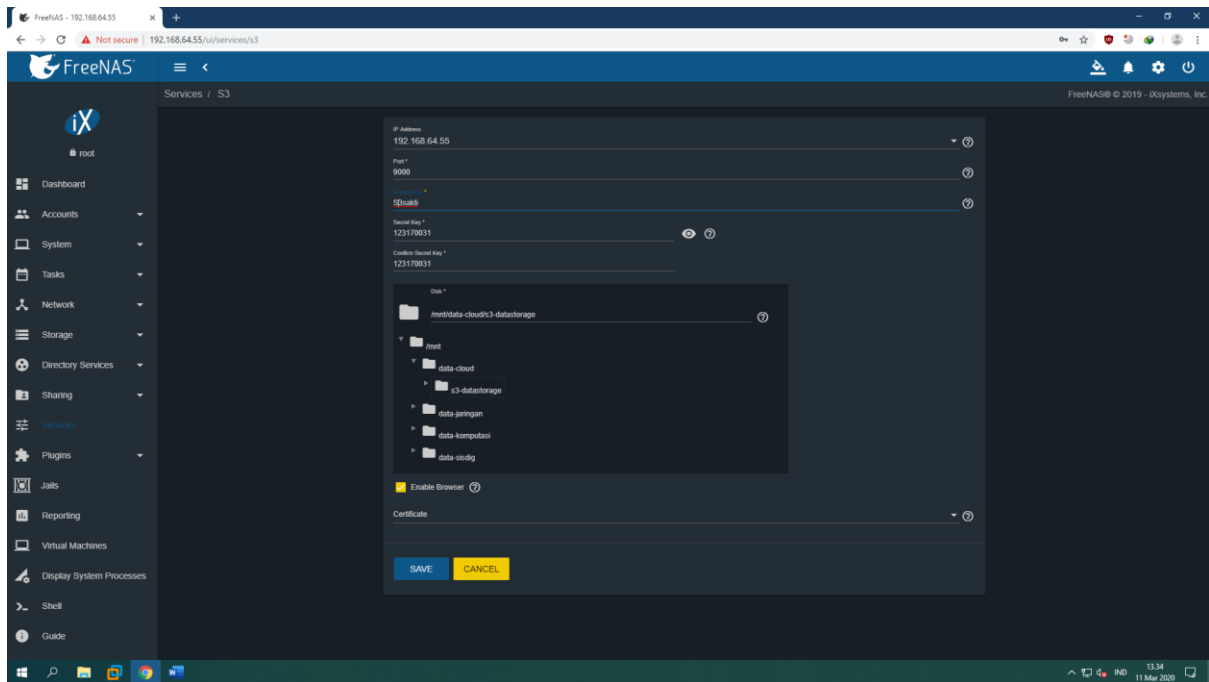
### 3. Isi nama s3-datastorage lalu save



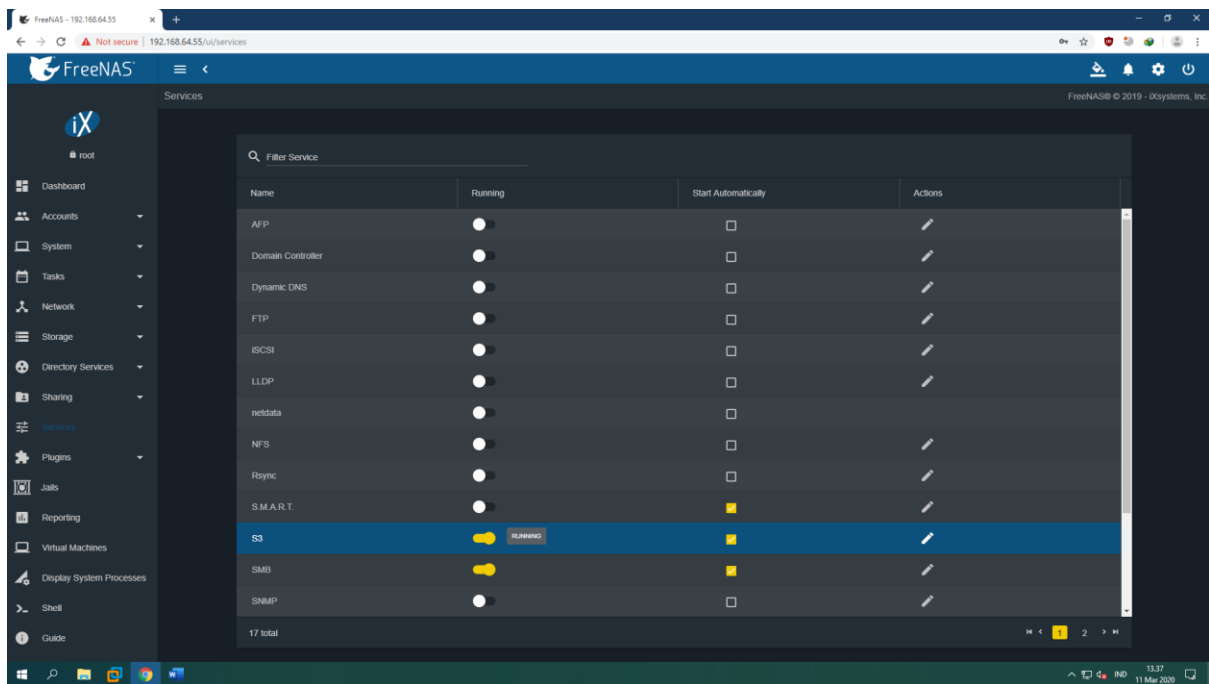
4. Masuk menu service lalu klik pencil (config)



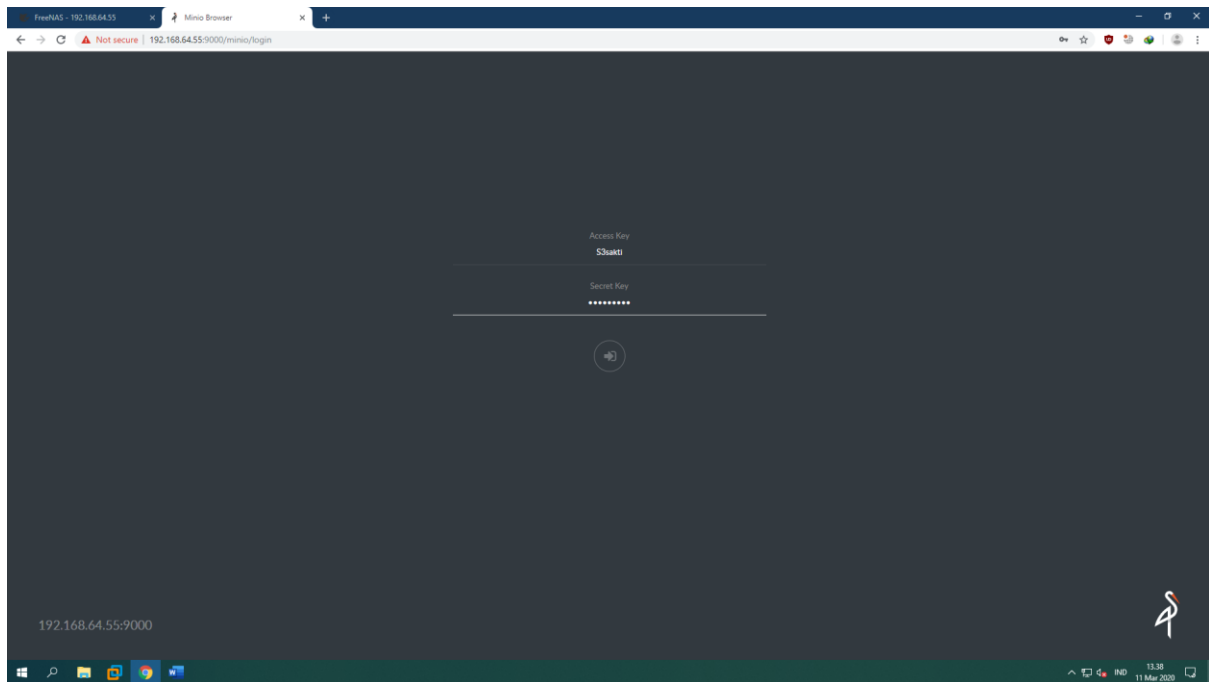
5. Config S3 dari IP Address dll sesuai pic lalu save



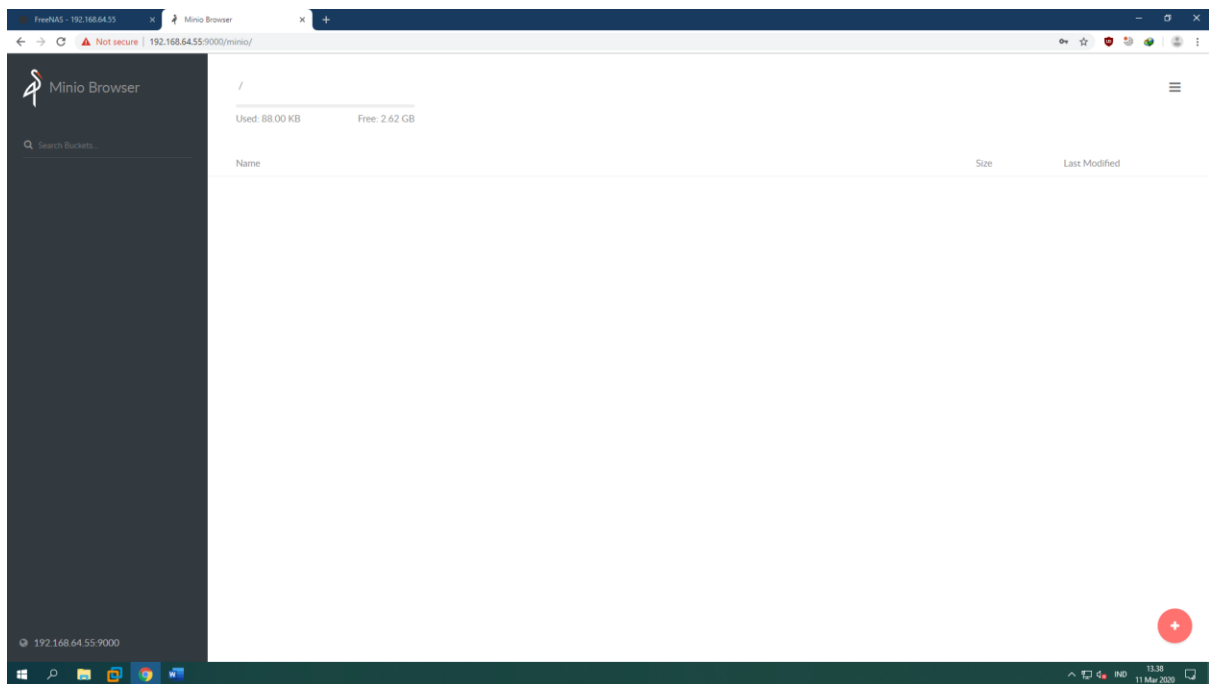
## 6. Start service dan start auto S3



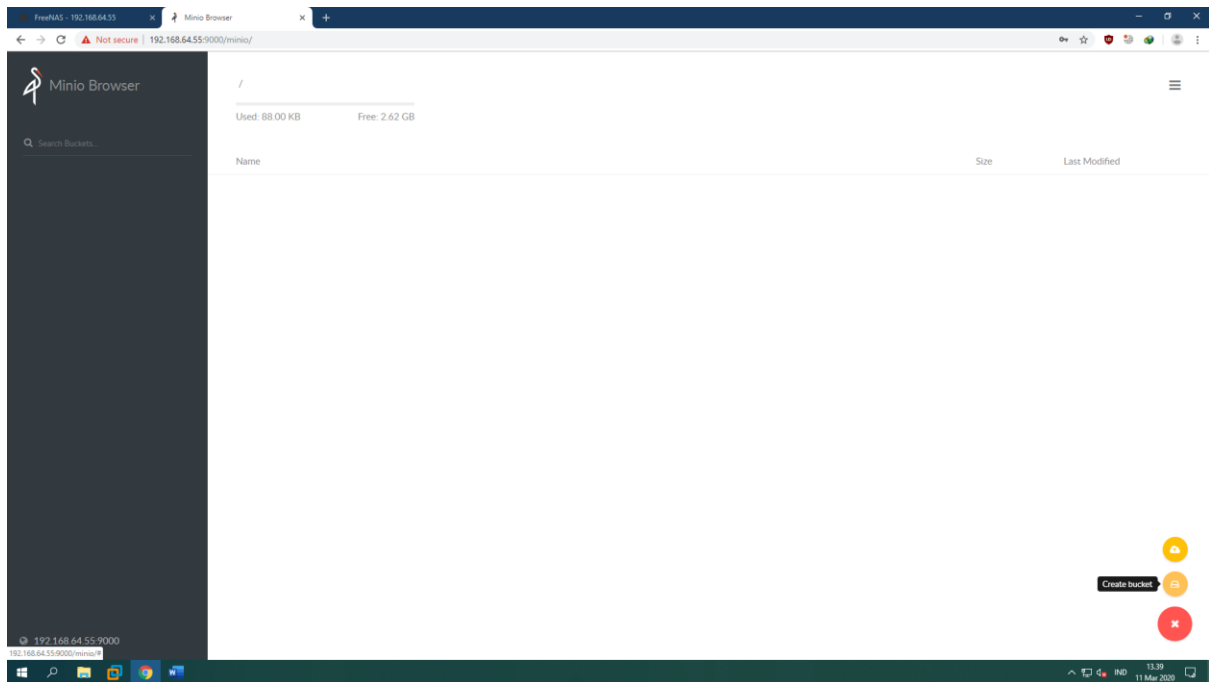
## 7. Akses S3 storage dengan IP:9000 (sesuai port yang di isi pd waktu config) lalu login



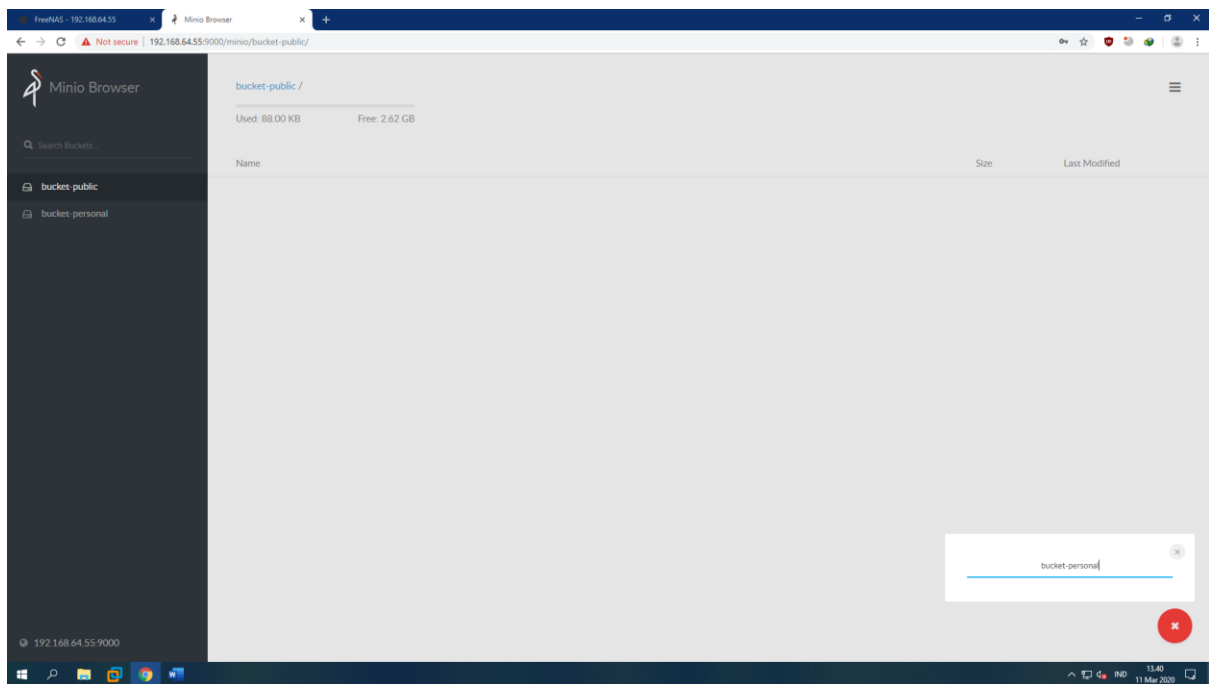
## 8. Tampilan setelah login



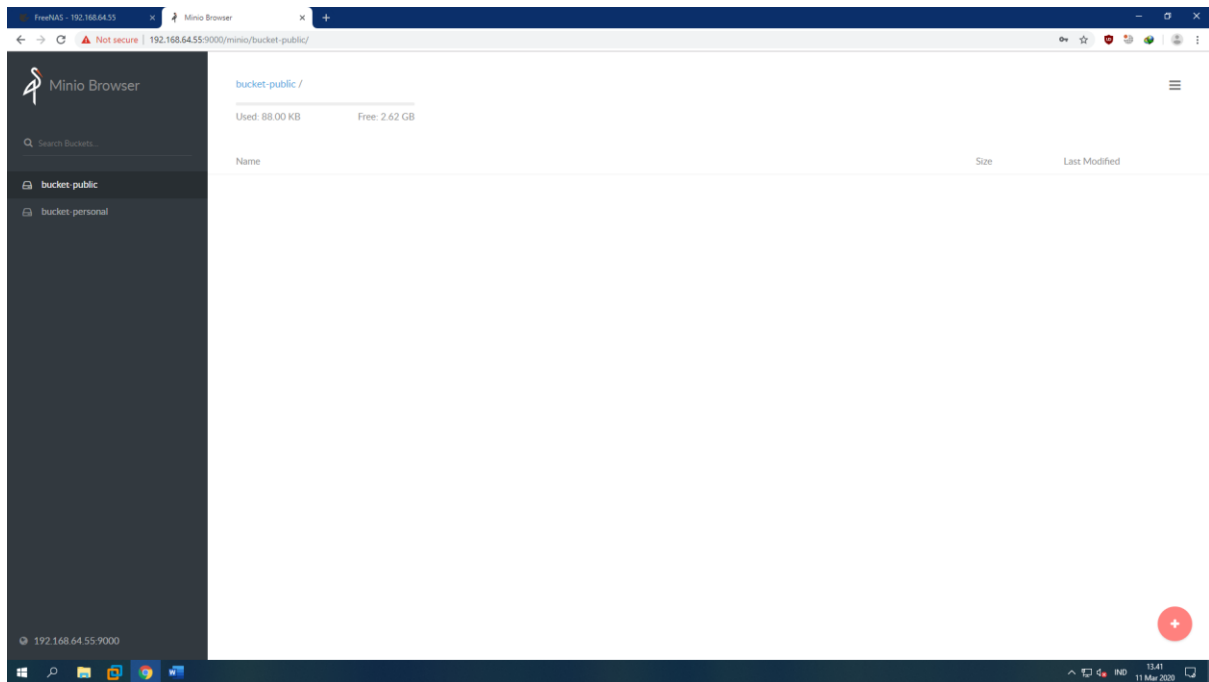
## 9. Add bucket



10. Beri nama bucket-personal dan bucket-public (tekan enter utk submit)

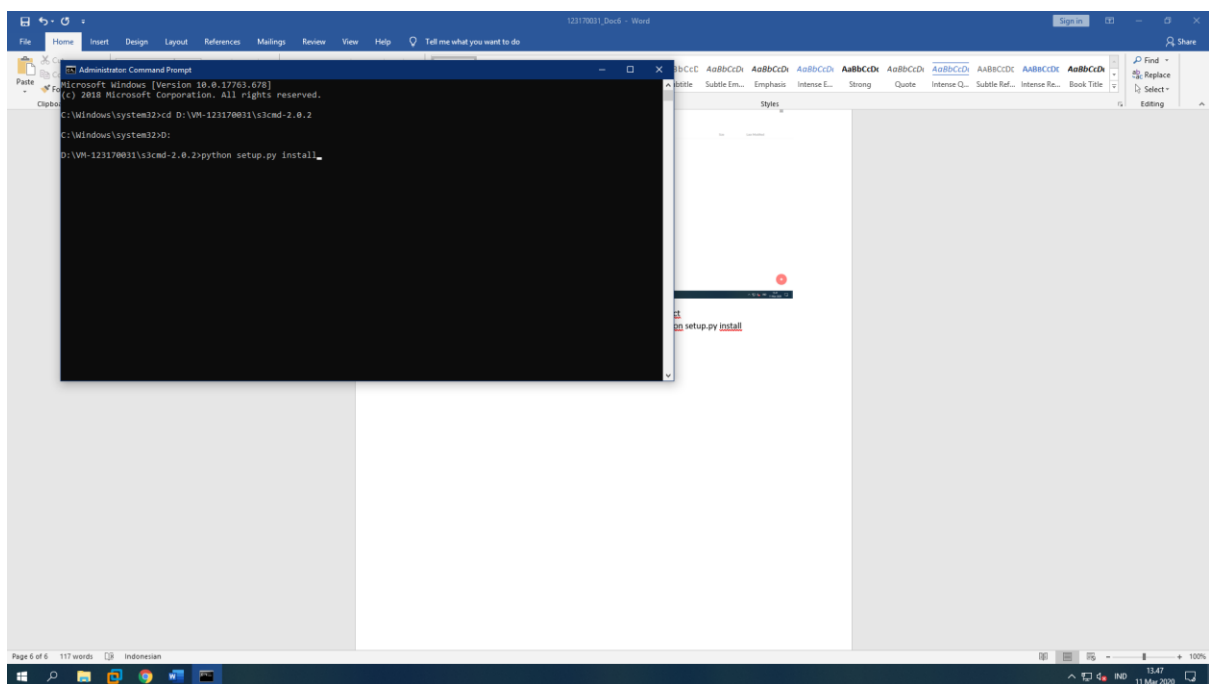


11. Hasil setelah add bucket



12. Download s3cmd di <http://s3tools.org/download> lalu extract

13. open cmd run as admin, masuk dir extract an td lalu run python setup.py install

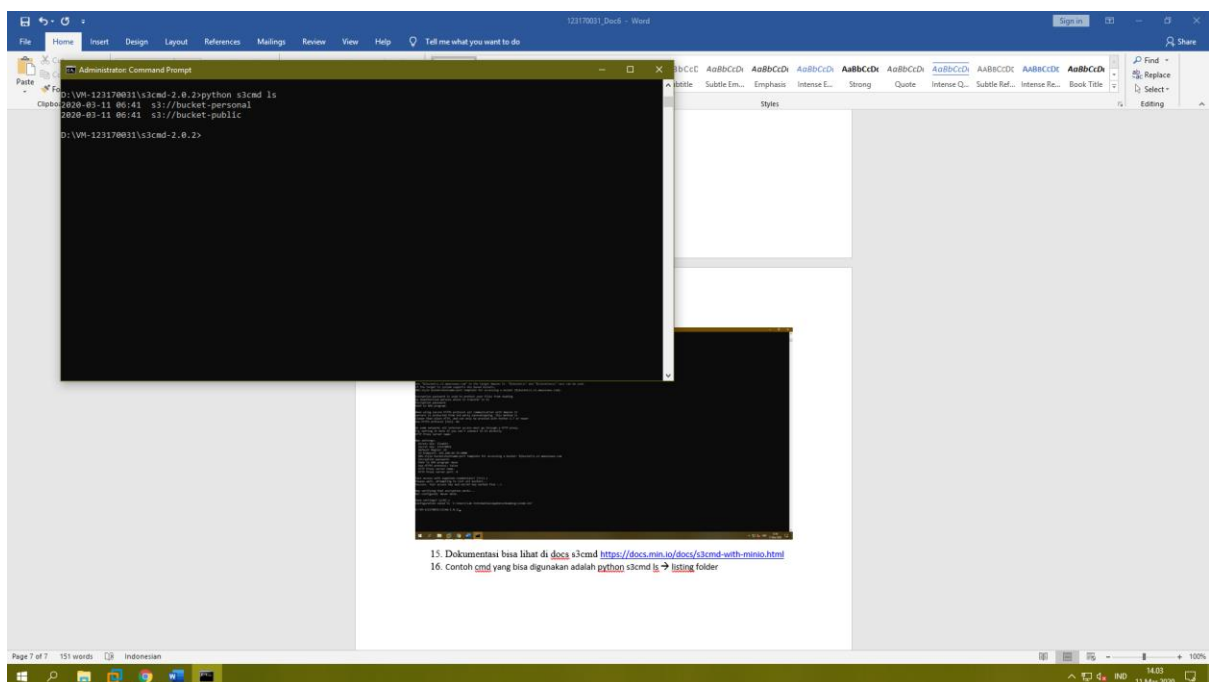


14. utk config run python s3cmd --configure lalu isikan sehingga akhirnya seperti pic

```
Administrator Command Prompt
D:\VM-123178031\s3cmd-2.0.2>python s3cmd --configure
ERROR: Option --preserve is not yet supported on MS Windows platform. Assuming --no-preserve.
ERROR: Option --progress is not yet supported on MS Windows platform. Assuming --no-progress.
Enter new values or accept defaults in brackets with Enter.
Refer to user manual for detailed description of all options.
Access key and secret key are your identifiers for Amazon S3. Leave them empty for using the env variables.
Access Key: S3uakt1
Secret Key: 123178031
Default Region [US]:
Use "s3.amazonaws.com" for S3 Endpoint and not modify it to the target Amazon S3.
S3 Endpoint [s3.amazonaws.com]: 192.168.64.55:9000
Use "%(bucket)s.s3.amazonaws.com" to the target Amazon S3. "%(bucket)s" and "%(location)s" vars can be used
if the target S3 system supports dns based buckets.
DNS-style bucket+hostname:port template for accessing a bucket [%s.s3.amazonaws.com]:
Encryption password is used to protect your files from reading
by unauthorized persons while in transfer to S3
Encryption password:
Path to GPG program:
When using secure HTTPS protocol all communication with Amazon S3
servers is protected from 3rd party eavesdropping. This method is
faster than plain HTTP, and can only be proxied with Python 2.7 or newer.
Use HTTPS protocol [Yes]: No
On some networks all Internet access must go through a HTTP proxy.
Try setting it here if you can't connect to S3 directly
HTTP Proxy server name:
New settings:
Access Key: S3uakt1
Secret Key: 123178031
Default Region: US
S3 Endpoint: 192.168.64.55:9000
DNS-style bucket+hostname:port template for accessing a bucket: %s.s3.amazonaws.com
Encryption password:
Path to GPG program: None
Use HTTPS protocol: False
HTTP Proxy server name:
HTTP Proxy server port: 0
Test access with supplied credentials? [Y/n] y
Please wait, attempting to list all buckets...
Success. Your access key and secret key worked fine :-))
Now verifying that encryption works...
Not configured. Never mind.
Save settings? [Y/N] y
Configuration saved to 'C:\Users\Lab Informatika\AppData\Roaming\s3cmd.ini'
D:\VM-123178031\s3cmd-2.0.2>
```

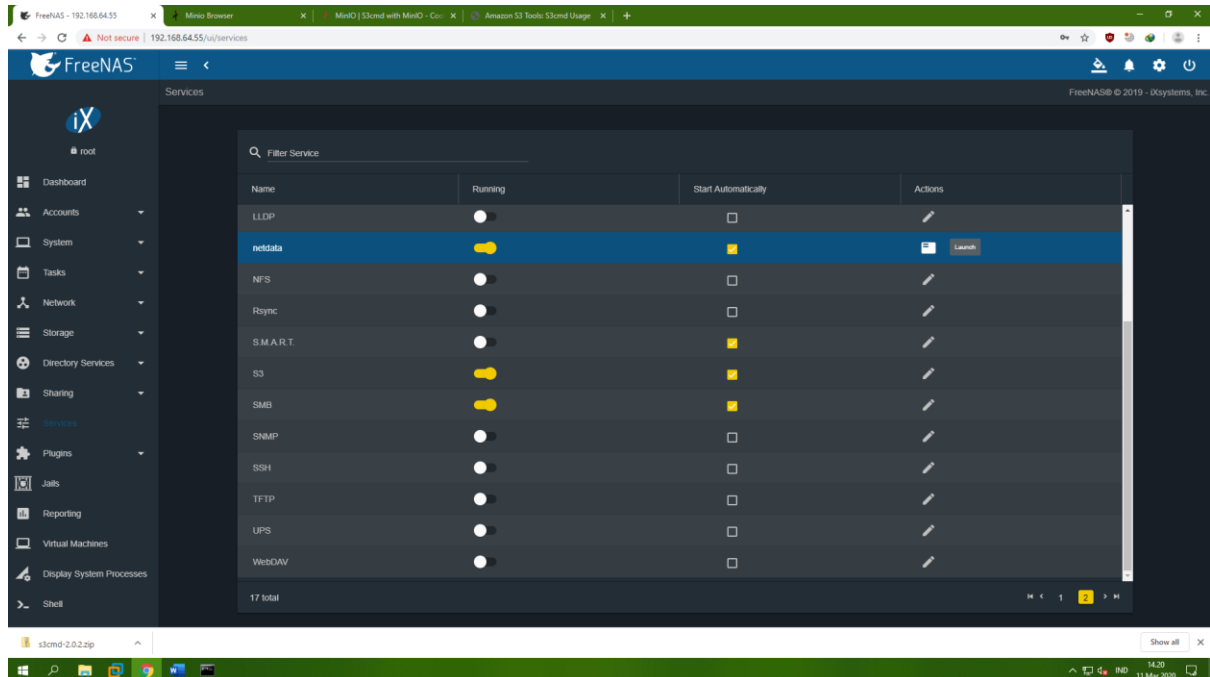
15. Dokumentasi bisa lihat di docs s3cmd <https://docs.min.io/docs/s3cmd-with-minio.html>

16. Contoh cmd yang bisa digunakan adalah python s3cmd ls → listing folder

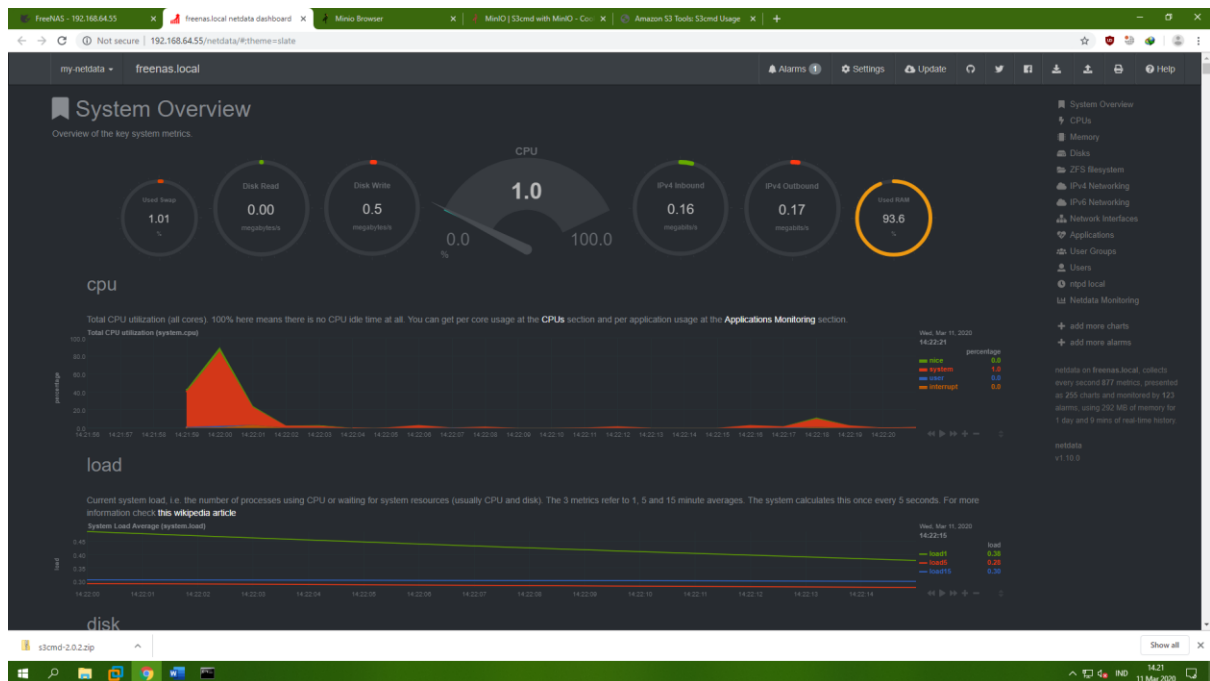


# Konfigurasi Netdata

## 1. Buka service lalu start netdata lalu launch



## 2. Tampilan netdata



## 3. Utk dokumentasi ada di netdata.cloud