

Set Up an S3 Service and Local Connection on FreeNAS® or TrueNAS®

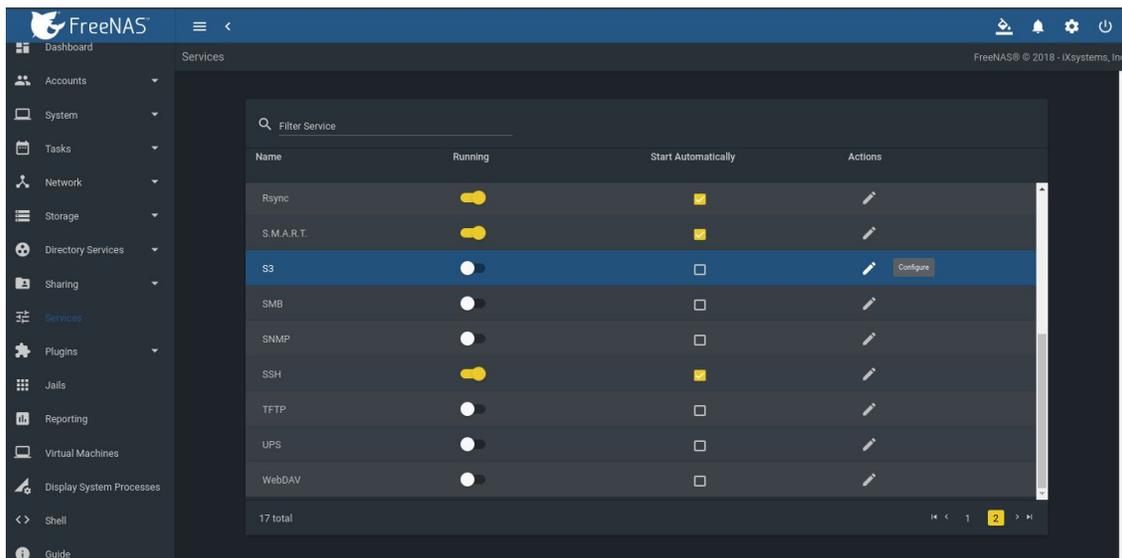
This tutorial describes how to start a local S3 service on FreeNAS and connect to it from a networked client system with the Minio Browser, s3cmd, and S3 Browser. The images show the latest FreeNAS 11.2 web interface and feature set. S3 support is also available on TrueNAS 11.1-U5 and later versions.

Background

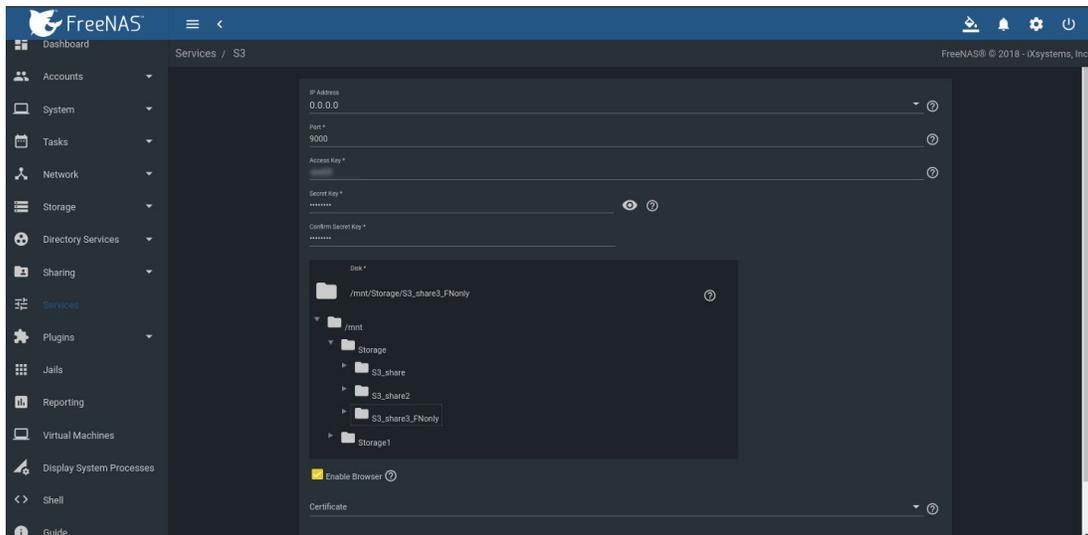
S3 is an object storage protocol used by many major cloud providers including Amazon Web Services™. On TrueNAS and FreeNAS, the service is another way to store files, and can be viewed with a web browser. Because S3 is the de facto standard for cloud-based storage, setting up an S3 service allows organizations or online application developers to use TrueNAS to replace or archive expensive cloud storage.

Setting up the S3 service

Go to **Services** -> **S3** and click on the pencil icon to edit.

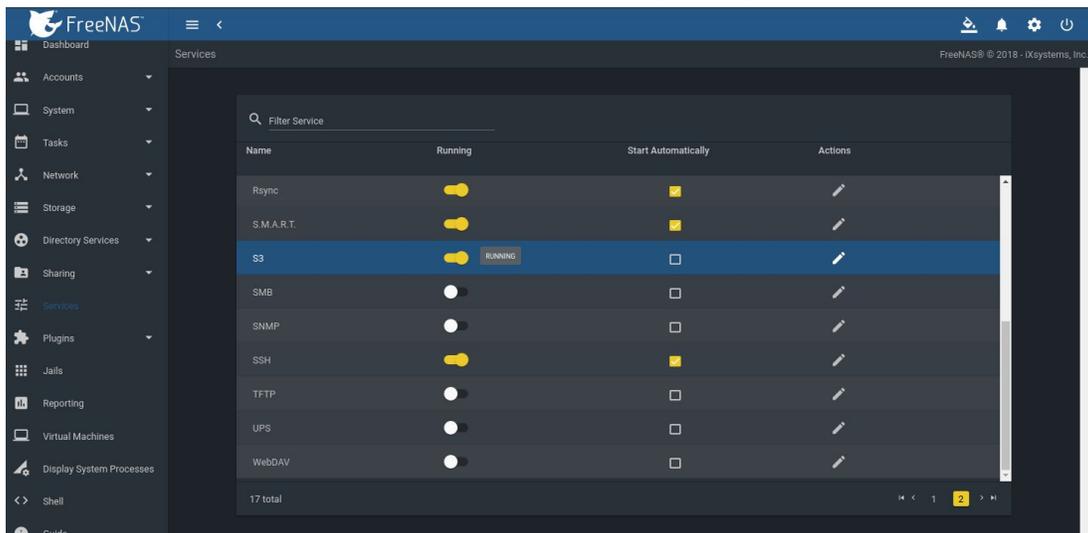


Set up the configuration inside this window.

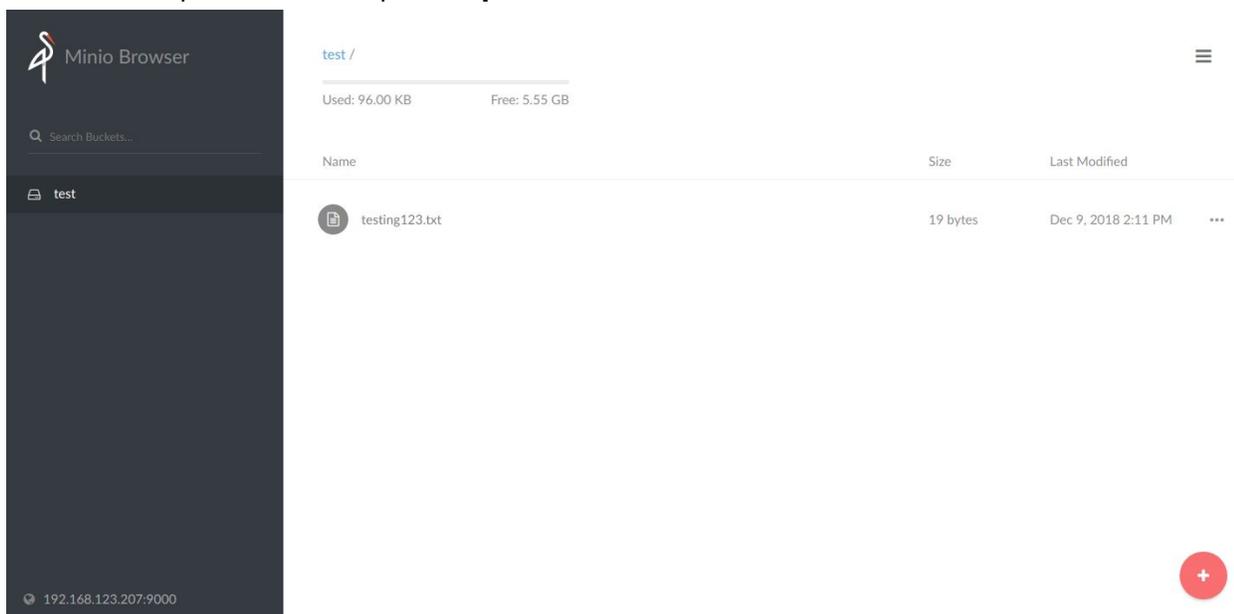


- Select IP address **0.0.0.0** to allow the service to listen on any IP address. Select the FreeNAS IP address to constrain it to a specific network.
- The default port is **9000**, but it can be changed as needed.
- Set an access key and secret key.
- Select a clean dataset. Files are managed by Minio as objects, and can NOT be mixed with other dataset files. New datasets can be created by going to **Storage -> Pools -> three dot menu -> Add Dataset** to create a new one.
- Choose to allow an S3 web browser (Minio Browser).
- Choose an SSH certificate for more secure connections.

Start the service and select whether to start automatically (on system boot).



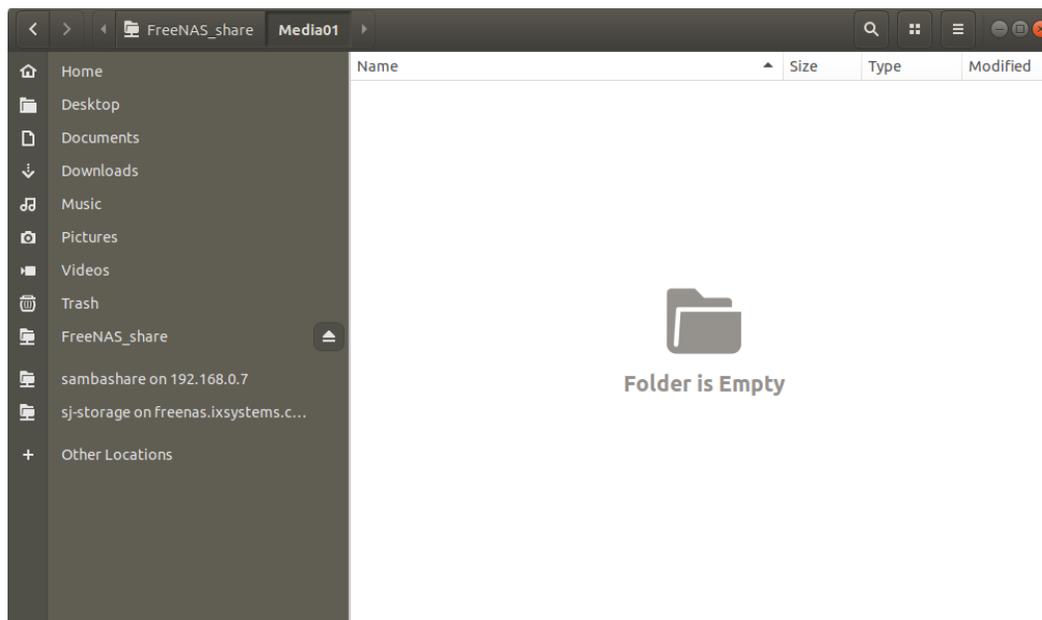
Test access to the Minio Browser by opening a web browser and typing the FreeNAS IP address with the TCP port. For example: **http://192.168.0.3:9000**



Buckets and files can be created and uploaded using the Minio Browser.

NOTE: Port **9000** must be allowed through the client firewall to permit bucket creation and file uploads.

NOTE: Files uploaded as S3 objects are NOT visible using standard file folders shared over standard file shares (NFS, AFP, SMB, FTP, etc.).



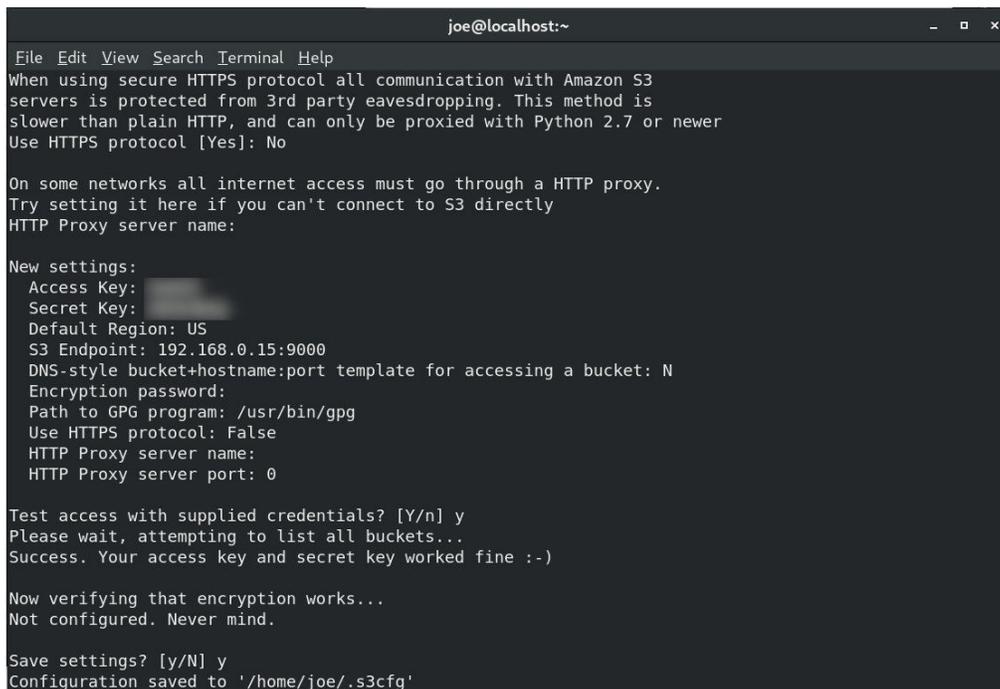
Setting Up s3cmd

Linux or macOS users must have the [s3cmd service](#) installed before beginning this setup. On Windows, users can also refer to [S3Express](#) for a similar command line experience.

Ubuntu can access the configuration by running **s3cmd --configure** to walk through important settings.

Enter the specified access key and the secret key. Under the **S3 Endpoint** enter the FreeNAS IP address followed by TCP port, and reply **N** to the DNS-style bucket+hostname.

Save the file. On Linux the default is in the home directory **~/s3cfg**.



```
joe@localhost:~  
File Edit View Search Terminal Help  
When using secure HTTPS protocol all communication with Amazon S3  
servers is protected from 3rd party eavesdropping. This method is  
slower 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: ██████████  
Secret Key: ██████████  
Default Region: US  
S3 Endpoint: 192.168.0.15:9000  
DNS-style bucket+hostname:port template for accessing a bucket: N  
Encryption password:  
Path to GPG program: /usr/bin/gpg  
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 '/home/joe/.s3cfg'
```

If the connection has any issues, open the config file again to clean it up. In Ubuntu use **nano .s3cfg** or **vi .s3cfg** or **gedit .s3cfg** depending on the preferred text editor. For other operating systems, .s3cfg file location and editing tools may vary.

Scroll down to the `host_bucket` area and make sure the **%(bucket)s** portion is removed and the address points to the `IP_address:TCP_port` for the system.

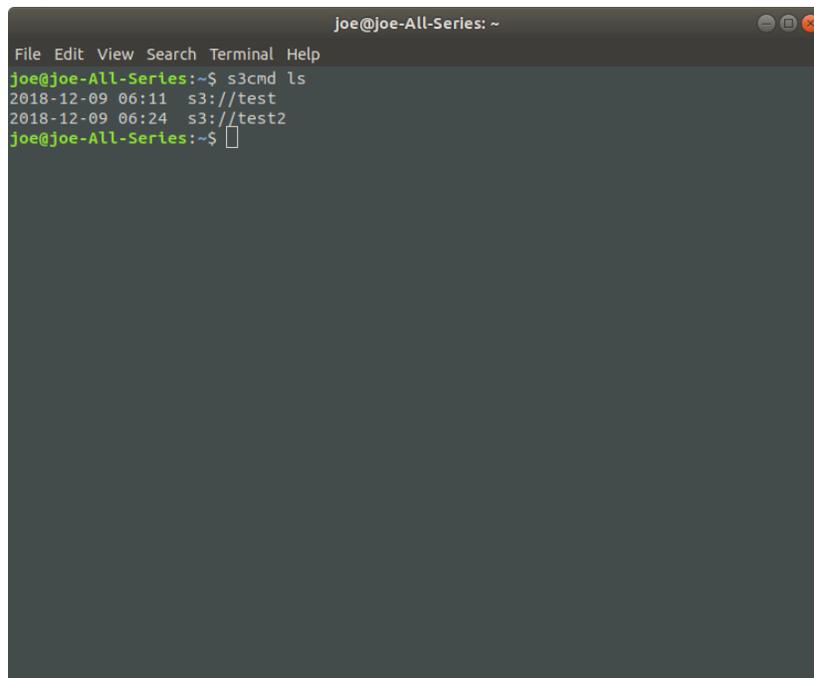
Right

Wrong

```
host_base = 192.168.123.207:9000  
host_bucket = 192.168.123.207:9000
```

```
host_base = 192.168.123.207  
host_bucket = %(bucket)s.192.168.123.207
```

Poll the buckets using **s3cmd ls**. The buckets created with the Minio Browser should be visible.

A terminal window titled 'joe@joe-All-Series: ~' with a menu bar (File, Edit, View, Search, Terminal, Help). The terminal shows the command 's3cmd ls' being executed, resulting in two lines of output: '2018-12-09 06:11 s3://test' and '2018-12-09 06:24 s3://test2'. The prompt 'joe@joe-All-Series:~\$' is visible at the end of each line.

```
joe@joe-All-Series: ~
File Edit View Search Terminal Help
joe@joe-All-Series:~$ s3cmd ls
2018-12-09 06:11 s3://test
2018-12-09 06:24 s3://test2
joe@joe-All-Series:~$
```

For more information on using Minio with s3cmd, see:

<https://docs.minio.io/docs/s3cmd-with-minio.html>

<https://s3tools.org/s3cmd>

Connect with S3 Browser

On Windows PCs, the S3 Browser is another convenient way to connect to the Minio S3 on a TrueNAS or FreeNAS system. To set it up, first install the [S3 Browser](#).

After installation completes, add a new account.

Add New Account
Enter new account details and click Add new account

Account Name:
New Account
Assign any name to your account.

Account Type:
Amazon S3 Storage
Choose the storage you want to work with. Default is Amazon S3 Storage.

Access Key ID:
Required to sign the requests you send to Amazon S3. see more details at <https://s3browser.com/keys>

Secret Access Key:
Required to sign the requests you send to Amazon S3. see more details at <https://s3browser.com/keys>

Encrypt Access Keys with a password:
Turn this option on if you want to protect your Access Keys with a master password.

Use secure transfer (SSL/TLS)
If checked, all communications with the storage will go through encrypted SSL/TLS channel

[Click here to sign up for Amazon S3.](#) Add new account Cancel

In the settings, select **S3 Compatible Storage** as the **Account Type**, then enter the Minio access point similar to the S3cmd setup (*FreeNAS_IP_address:9000* or other port if set differently). Select the SSL settings appropriate for the particular setup. The default assumes SSL in S3 Browser, but for a LAN attached session, this may or may not have been set.

Edit Account
Edit account details and click Save changes

Account Name:
Storage
Assign any name to your account.

Account Type:
S3 Compatible Storage
Choose the storage you want to work with. Default is Amazon S3 Storage.

REST Endpoint:
192.168.0.9:9000
Specify S3-compatible API endpoint. It can be found in storage documentation. Example: rest.server.com:8080

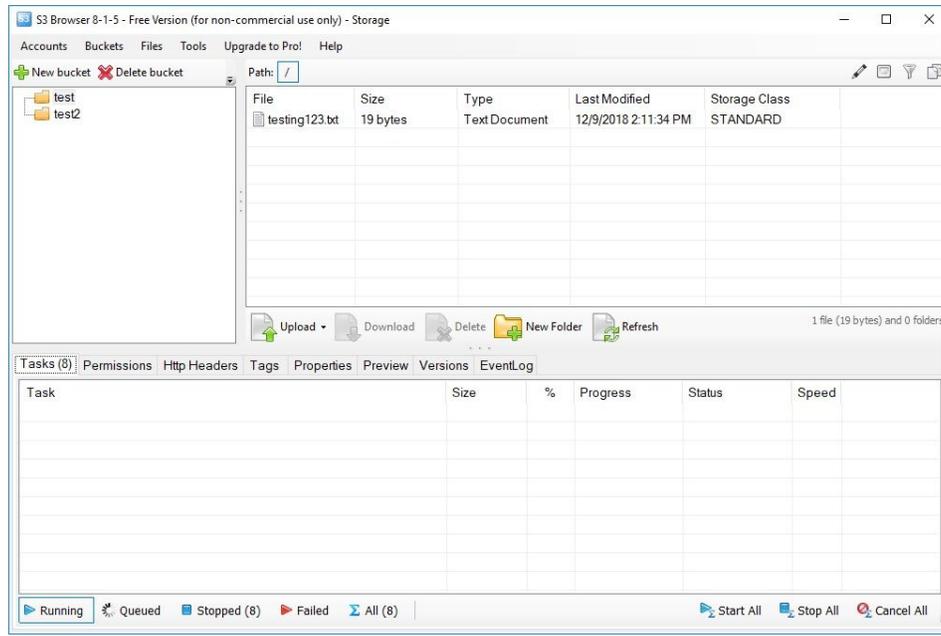
Signature Version:
Signature V2
Choose the supported signature version. Default value is Signature V2.

Access Key ID:
Required to sign the requests you send to Amazon S3. see more details at <https://s3browser.com/keys>

Secret Access Key:
••••••

[Click here to sign up for Amazon S3.](#) Save changes Cancel

It is possible to access, create new buckets, or upload files to created buckets.



We hope that this guide will help you quickly set up and attach an S3 object storage manager of your choice. For any questions or inquiries, please [contact us](#).