napp-it

napp-it Encryption and Keyserver

Checklist

published: 2023-Mar-28 (c) napp-it.org

Encryption, basic setup

1. Encryption with passphrase

This is the default encryption method. You can lock/unlock a filesystem with a passphrase,
even when you created a filesystem with file or webbased keys, so backup the passphrases as this is your first fallback option if you forgot the key or the file or webbased keys are lost.

2. Encryption with filebased keys (L1:L1)

This is a encryption method where the unlock key (a passphrase) is stored on a ZFS pool (can be a pool on a removeable USB stick or disk or a remote iSCSI target. If the key is accessble a filesystem can be unlocked when you click on the „locked" state of a filesystem. To enable filebased encryption set the filepath to your keys in About > Settings ex tank/keydata (L1)

2a. Encryption with filebased key-split (L1:L2)

This is a encryption method where the unlock key (a passphrase) is stored on a ZFS pool (can be a pool on a removeable USB stick or disk or a remote iSCSI target in two parts where each part is on a different location ex pool1/usb1 and pool2/usb2. If both parts of the the key are accessble a filesystem can be unlocked when you click on the „locked" state of a filesystem. To enable splitted filebased encryption set the filepath to your keys in About > Settings ex tank/keydata (L1) and scondary filesystem (L2)

3. Encryption with webbased keys (W1:W1)

This is a encryption method where the unlock key (a passphrase) is stored on a webserver (another napp-it server). To allow webbased keys, add the server url in About > Settings (first webserver, W1) ex https://ip:82 and add a filepath for webserver keys ex tank/keydata (can be same location as filebased keys. These passphrses are delivered remotely via http(s). Additionally allow webbased keys and keyserver in About > Settings.

Next step is to add a client config that enables keyaccess fo a client with a client id. This is done in menu Services > Keyserver > Client: add with the hostname of a client. Copy the client id and insert it in
About > Settings under Access ID.

Check:
Services > Keyserver (every field green) and
Flesystems > Encryption (state of L1,L2, W1,W2) (all ok)

Now you can create encrypted filesystems with L1:L1 (Keys on L1), splitted keys (L1:L2) or webbased keys (W1:W1) where keys are on keyserver 1. A special option is a keysplit L1:W1 or W1:W2 where one half of a key is on pool and the other half on a webserver or keys are splitted between webservers.

3a. Move keys (Local <-> keyserver -> manual unlock)

If you open the keyserver folder ex tank/keydata you will find a folder local and webserver with the key parts.
A simple move and the keys access switch between local and keyserver. Additionally you can always unlock a filesystem when you enter the passphrase manually in the unlock field.

4. Keyserver failover

Currently there is no automatic failover from keyserver 1 (W1:W1) to a keyserver 2 (W1*:W1*). This is a planned feature. Currently you can create a second napp-it instance, set there a keyserver folder and enable the keyserver. Then copy over the content of the keyserver folder with the client part from server 1 to server 2. For a failover enter the ip of the active keyserver in About > Settings as keyserver 1 (W1). Use the field W1* to remember a second keyserver 2.