NAS Installation - Synology DSM 7.4

KMIP for key management

- Follow the guide to install KMIP on a Synology NAS server and client

Certificates

1. The default, out-of-the-box self-signed Synology certificate will fail on DSM 7.4 and later, which hardened the certificate requirements. You will generate matching certificates from an official Synology script, which will be installed alongside the default certificates, and are valid for 10 years. These certificates also work for Synology clients, when added to a KMIP Server (PyKMIP) not hosted on a synology NAS.
2. Login to your NAS on the command line with SSH and elevate to root
3. Download Synology's official KMIP certificate script:

   ```
   wget
   supweb.synology.com/support_web/kc_tool/how_to_gen_cert_for_kmip_servic
   es/gen_kmip_certs.sh
   ```

4. Run the script as root:

   ```
   bash gen_kmip_certs.sh kmip_certs
   ```

   The second parameter *kmip_certs* is the name of a shared folder the script will create to store the certificates

5. Upload the generated scripts in `/volume1/kmip_certs` to your local computer you use to access your DSMs through your web browser, after which you can remove the shared folder and it's content
6. The script will generate the following certificates:

   ```
   ca-key.pem
   ca.pem
   client-fullchain.pem
   client-key.pem
   client.pem
   server-fullchain.pem
   server-key.pem
   server.pem
   ```

DSM as Server

1. go to *Control Panel > Security > Certificate*
2. Click *Add*, choose *Import Certificate*, and upload:
   - Private key: `server-key.pem`

    - Certificate: `server.pem`
    - Leave Intermediate certificate empty
3. Click Settings (in the Certificate tab), find the *KMIP dropdown menu*, select this new server certificate, and click OK
4. Go to *Control Panel > Security > KMIP* and select *Set as remote key server*
5. Under *Manage Client Connection*, click *Manage > Add*
6. Upload the client files you generated:
    - Client certificate: `client.pem`
    - Certificate authority: `ca.pem`
7. Add a port forward for port 5696 to your server NAS

DSM as Client

1. go to *Control Panel > Security > Certificate*
2. Click *Add*, choose *Import Certificate*, and upload:
    - Private key: `client-key.pem`
    - Certificate: `client.pem`
    - Leave Intermediate certificate empty
3. Click Settings (in the Certificate tab), find the *KMIP dropdown menu*, select this new client certificate, and click OK
4. Go to *Control Panel > Security > KMIP* and select *Set as remote key client*
5. Enter the server's IP address and port 5696
6. Upload the certificate authority file `ca.pem` and click **Next**. Wait until you see the connection is successful.
7. Now you need to go to **Storage Manager –> Storage** and click *Global Settings*. Scroll down to **Encryption Key Vault** and click *Reset* (important!) to make the switch to the KMIP Server permanent and move the encryption keys.

How to gain access to encrypted volumes when the KMIP Server was unavailable during DSM boot

- If you can re-establish connection to the KMIP Server you can do the following:
    1. SSH into DSM
    2. if you want to continue using the KMIP Server:

    ```
    reboot
    shutdown -r now
    ```

    3. if you do not want to continue using the KMIP Server:

    ```
    sudo /usr/syno/sbin/synoencvolume --auto-unlock-get-keys
    ```

    4. Log into DSM and open Storage Manager. You can now access DSM through it's web interface, but you cannot access your files.
    5. Reset the Encryption Key Vault in the *Global Settings* of the **Storage Manager** using the recovery key to disconnect your NAS from the KMIP Server.
    6. If your locked volume is not the same volume where your user home directories reside you can go to the **Storage Manager** and select the locked volume, then click the ellipsis (...) icon, and select *Unlock*. Upload your `.rkey` recovery file. The system will prompt you to enter a new vault password to recreate and repair the local key vault.

Recover an encrypted volume using an SSH shell

- If you can not re-establish connection to the KMIP Server you can do the following:
  1. Identify the Target Device Node
     - Synology layers its storage using Linux mdadm (RAID) and Logical Volume Management (LVM). You need to find the logical volume path:

       ```
       sudo lvdisplay
       ```

     - Look for your volume path, e.g. `LV Path /dev/vg1/volume_1`
  2. Unlock the LUKS Container
     - Depending on what credentials you have, choose Option A or Option B
     - Option A: Using the Passphrase. Pass the LVM path to cryptsetup to open it. This will prompt you for the password:

       ```
       sudo cryptsetup luksOpen /dev/vg1/volume_1 mapped_volume
       ```

     - Option B: Using the Recovery Key (.rkey file). If you have the `.rkey` file saved on a USB drive or transferred via SSH to `/tmp/volume1.rkey`, use:

       ```
       sudo cryptsetup luksOpen /dev/vg1/volume_1 mapped_volume --
       key-file /tmp/volume1.rkey
       ```

     - Note: mapped_volume is just a temporary virtual name you assign for the next step.
  3. Mount the Filesystem
     - Synology volumes typically use the Btrfs or ext4 file systems. Create a temporary folder and mount the newly decrypted mapping:

       ```
       sudo mkdir -p /mnt/recovery
       mount /dev/mapper/mapped_volume /mnt/recovery
       ```

  4. Access and Rescue Your Data
     - Your data is now fully unencrypted and accessible in plain text at `/mnt/recovery`. You can use command-line tools like `cp`, `rsync`, or `tar` to copy your files off to an external drive or another server.

How to Regenerate and Download a Recovery Key

1. Open **Storage Manager** in Synology DSM
2. Go to **Storage** and click on your encrypted volume
3. Click the *Settings* button (or the three dots/action menu next to the volume)
4. Locate the **Recovery Key** section
5. Click *Regenerate*
6. Enter your Vault Password when prompted to authorize the action
7. The new recovery key file (`.rkey`) will download automatically to your computer's default download folder

Links

- Updated security and certificate guidelines for DSM 7.4

- Setting up a KMIP server with DSM 7.4
- Random Password Generator