NAS Installation - Synology DSM 7.4

Upgrade from DSM 6.4

- First upgrade to DSM 7.0 through *Control Panel*
- Go to the Synology Download Center, *Select product type* and *Select your Synology Product*, then *Select DSM version* currently installed and the latest DSM version offered for this product as a target DSM version
- Upload the downloaded update file in *Control Panel –> Update & Restore –> Manual DSM Update* and start the update
- The update should run without issues, after which there are a few extensions which are obsolete and which you can uninstall

KMIP for key management

- Follow the guide to install KMIP on a Synology NAS server and client
- What this guide does not mention is how to generate working certificates for 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.
    1. The default, out-of-the-box self-signed Synology certificate will fail on DSM 7.4
    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_s
        ervices/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
```

7. On the server NAS
   - go to *Control Panel* > *Security* > *Certificate*
   - Click *Add*, choose *Import Certificate*, and upload:
     - Private key: `server-key.pem`
     - Certificate: `server.pem`
     - Leave Intermediate certificate empty
   - Click Settings (in the Certificate tab), find the *KMIP dropdown menu*, select this new server certificate, and click OK
   - Go to *Control Panel* > *Security* > *KMIP* and select *Set as remote key server*
   - Under *Manage Client Connection*, click *Manage* > *Add*
   - Upload the client files you generated:
     - Client certificate: `client.pem`
     - Certificate authority: `ca.pem`
   - Add a port forward for port 5696 to your server NAS
8. On the client NAS
   - go to *Control Panel* > *Security* > *Certificate*
   - Click *Add*, choose *Import Certificate*, and upload:
     - Private key: `client-key.pem`
     - Certificate: `client.pem`
     - Leave Intermediate certificate empty
   - Click Settings (in the Certificate tab), find the *KMIP dropdown menu*, select this new client certificate, and click OK
   - Go to *Control Panel* > *Security* > *KMIP* and select *Set as remote key client*
   - Enter the server's IP address and port 5696
   - Upload the certificate authority file `ca.pem` and click **Next**, they client will not attempt to connect to the server

Links

- Updated security and certificate guidelines for DSM 7.4
- Setting up a KMIP server with DSM 7.4