Quantum®

# StorNext NAS with Apple Open Directory

**Version** 1

## Configuration procedures

The SN-NAS module provides the ability to integrate a StorNext appliance with directory services, which provides user authentication for accessing NAS shares.

These instructions can be used to generate a Kerberos keytab so that the SN-NAS can operate in an Apple Open Directory environment which is not currently leveraging Kerberos for authentication.

Once created, the Administrator can import the keytab file described in the StorNext Appliance NAS Configuration Guide.

This operation does not change the existing authentication methods utilized in the envrionment, but enables the bare minimum for SN-NAS to utilize the native Kerberos features of Apple Open Directory.

## OS X 10.5 - 10.9 Specific

### Generating a Kerberos Keytab File

Complete the following steps to generate a keytab file for the NAS service principal.

**Note** case is important

1. Log in to the Apple Open Directory Server used to authenticate user access to the StorNext appliance

2. In the terminal while logged in as root, type

```
kadmin -l
```

   (The kadmin shell opens)

3. Create the service principal in the Kerberos Database

```
add --random-key cifs/NASfqdn@REALM
```

4. Verify that the principal was created by reading its entry in the Kerberos Database

```
get cifs/NASfqdn
```

5. Create a keytab containing the principal

```
ext_keytab -k krb5.keytab.NAS cifs/NASfqdn@REALM
```

6. Exit the kadmin program

```
quit
```

7. Confirm that the file krb5.keytab.NAS is present in the working directory

## OS X 10.10 - 10.11 Specific

### Generating a Kerberos Keytab File

Complete the following steps to generate a keytab file for the NAS service principal.

Note that case is important.

1. Log in to the Apple Open Directory Server used to authenticate user access to the StorNext appliance

2. In the terminal, as root, type

```
krbservicesetup -x cifs cifs/NASfqdn@REALM
```

   An output of ktutil: remove: Key table entry not found is normal.

3. In the terminal, as root, type

```
kadmin -l
```

4. Verify that the principal was created by reading its entry in the Kerberos Database

```
get cifs/NASfqdn@REALM
```

5. Create a keytab containing the principal

```
ext_keytab -k krb5.keytab.NAS cifs/NASfqdn@REALM
```

6. Exit the kadmin program

```
quit
```

7. Confirm that the file krb5.keytab.NAS is present

## Importing the Keytab File

1. Copy the newly generated keytab file as krb5.keytab in /var/upgrade on the NAS computer

2. Log in the appliance in the SN-NAS CLI as sysadmin to import the keytab file from /var/upgrade

   (a) Note that the keytab file must be named 'krb5.keytab' in order for SN-NAS to import it

```
auth import keytab
```

3. Configure the ldap client

   (a) The following is the syntax for the command, substitute your actual Open Directory server and Kerbeors realm

```
auth config ldap keytab OpenDirectoryMasterFQDN REALM
```

4. confirm the configuration

```
auth show
```

## Client/Workstation Kerberos Config

Is a manual kinit required or does it happen automataically?

## Removing the configuration

1. Log in the appliance in the SN-NAS CLI

   ```
   auth reset config
   ```

2. Log in the OD master and open a kadmin session as root

   ```
   kadmin -l
   ```

3. Confirm that the principal is in the Kerberos database

   ```
   get cifs/NASfqdn@REALM
   ```

4. Remove the NAS principal from the Kerberos database

   ```
   del cifs/NASfqdn@REALM
   ```

5. Confirm that the principal is out of the database

   ```
   get cifs/NASfqdn@REALM
   ```

## Additional Information

- Hostname: the computer name, ex: nas
- Fully Qualified Domain Name (fqdn): the full name of the computer including the domain and the tld: nas.domain.com
- The Open Directory Domain: This is the domain on witch the directory service act upon
  - It is usually expressed as domain.tld.
  - In some environments it will be expressed as opendirectorymastername.domain.tld
  - That information can be extracted from the Search Policy in Directory Utility or by running the following coming on a bound computer in the domain

    ```
    dscl localhost read Search SearchPath
    ```

- Kerberos Realm: the domain on which Kerberos acts upon.
  - It is usually derived from the Open Directory Domain
  - It is usually expressed as DOMAIN.TLD (caps are important) or, depending on the Open Directory domain, ODMASTER.DOMAIN.TLD
  - That information can be extracted by doing klist on a logged in OD user or by doing

    ```
    dscl localhost -read /LDAPv3/TheOpenDirectoryDomain/Config/KerberosKDC RealName
    ```