Enable NFSv4 on VNX

To enable NFSv4 on your up-to-date *(post VNX OE for File v7.1)* VNX Unified storage system and configure a datamover to mount a filesystem to allow for NFSv4 access with a MIXED access policy, the following steps serve as a concise guide. NFSv4 cannot be done via Unisphere.

Log onto control station as **nasadmin** user via SSH using PuTTY.

START NFSv4 Server on VNX
server_nfs server_2 -v4 -service -start

SET DOMAIN NAME to *nfsv4.domain (change as required)*
server_param server_2 -facility nfsv4 -modify domain -value nfsv4.domain

LIST NFSv4 DOMAIN INFO
server_param server_2 -facility nfsv4 -info domain

LIST NFSv4 INFO
server_param server_2 -facility nfsv4 -list

MOUNT NFS_TEST_2 on server_2 for NFSv4 access
server_mount server_2 -option accesspolicy=MIXED NFS_TEST_2 /NFS_TEST_2

TRANSLATE existing, mounted NFS filesystem from NATIVE access policy to MIXED access policy
nas_fs -translate NFS_TEST_2 -access_policy start -to MIXED -from NATIVE

DISPLAY NFSv4 CLIENT CONNECTIONS
server_nfs server_2 -v4 -client -list

NFSv4 requires UNICODE enabled on DM. Check…
server_cifs server_2 | grep I18N
I18N mode = UNICODE

DISPLAY NFSv4 STATUS
server_nfs server_2 -v4

It's highly likely that if you require NFS v4, then you'll also need to authenticate access, using a UNIX based Kerberos DC. The following notes cover the configuration steps involved. Please note that this section below is still a work in progress and you should refer to the official EMC documentation for a complete set of instructions with examples.

SECURE NFS (using UNIX Kerberos Authentication)

CONFIGURE THE KERBEROS REALM
server_kerberos server_2 -add realm=<realm-name>,kdc=<fqdn_kdc_name>,kadmin=<kadmin_server>,domain=<domain_name>,defaultrealm
Note realm,kdc, kadmin,domain should all be entered as fqdn's

VERIFY THE RESULTS
server_kerberos server_2 -list

SET THE SECURE NFS SERVICE INSTANCE
server_nfs <datamovername> -secnfs
Note server_2 is set already during VNX installation.

CHANGE THE SECURE NFS SERVICE INSTANCE
server_nfs <newdatamovername> -secnfs -principal -delete nfs@server_2
Note This is only required if you change the default datamover hostname from server_2 to e.g. Ingbe245
server_nfs <newdatamovername> -secnfs -principal -create nfs@<server>
Note <server> is type of the realm, and needs to be entered twice, once with short name, e.g. Ingbe245 and once more with fqdn

STOP AND START THE NFS SERVICE
server_nfs server_2 -secnfs -service -stop

server_nfs Ingbe245 -secnfs -service -start

DETERMINE IF KEYTAB FILE EXISTS ON DATAMOVER
Copy **/.etc/krb.keytab** file (if it exists) to the Kerberos KDC.

CREATE NFS KERBEROS SERVICE PRINCIPALS
Note. The kadmin steps are performed on the Kerberos KDC, not the VNX
kadmin: addprinc=randkey nfs/Ingbe245
kadmin: addprinc=randkey nfs/Ingbe245.fqdn.local

VERIFY THAT THE PRINCPALS HAVE BEEN ADDED
kadmin: listprincs

GENERATE SECURITY KEYS
kadmin: ktadd -k <keytab_file_path> nfs/ <name>
<keytab_file_path> = location of key file
<name>=name of previously created service principal e.g. nfs/Ingbe245

COPY KEYTAB FILE
Copy the **krb5.keytab** file from Kerberos KDC to the Data Mover by using FTP and the **server_file** command.
Note. EMC Common Anti-Virus Agent (CAVA) is also configured using the **server_file** command to place and displace the viruschecker.conf file. There are notes on that here but to save you the trouble, the command for your convenience is…

server_file server_2 -get krb5.keytab krb5.keytab

server_file server_2 -put krb5.keytab krb5.keytab
VIEW THE KEYTAB FILE
server_kerberos Inbe245 -keytab

MAP USER PRINCPAL NAMES TO UIDs
VERIFY THE TYPE OF MAPPING SERVICE USED BY SECURE NFS
server_nfs <datamovername> -secnfs -mapper -info

USE AUTOMATIC MAPPING
server_nfs <datamover_name> -secnfs -mapper -set -source auto

MONITOR INBOUND CONNECTIONS FROM NFSV4 CLIENTS

server_nfs server_2 -v4 -client -list