NetApp Storage Admin SMB/CIFS ACLs Guide

Overview

This document is to enable Storage Administrators to properly configure a NetApp core filer for enabling SMB/CIFS ACL-enforced access to an NTFS security style share for Windows clients. After completing the steps in this guide, the process continues in the FXT Admin SMB/CIFS ACLs Guide and the AD Administrator CIFS ACLs Guide. Choose one of the two checklists depending on whether using a new volume or an existing volume.

NetApp Checklist - New volume

1. Create a new volume.
2. Change to NTFS security style.
3. Modify volume export policy to provide root access for FXT Cluster IP addresses and Client IP addresses. Verify using `exportfs -q /<VOLNAME>`
4. Create a CIFS share.
5. Verify volume security style is NTFS using `fsecurity show /<VOLNAME>`.
6. Enable the NFS root user to bypass ACL processing.
7. Map root UNIX user to the Active Directory user with Full Control permissions, usually Domain Administrator account.

NetApp Checklist - Existing volume

1. Verify volume security style is NTFS using `fsecurity show /<VOLNAME>`.
2. Verify that the export is configured to enable NFS read/write and root access from the Avere client and cluster IP addresses using `exportfs -q /<VOLNAME>`
3. Enable the NFS root user to bypass ACL processing.
4. Map root UNIX user to the Active Directory Domain Administrator account.

Configuring a volume on the NetApp Core filer

Configure a volume on the core filer

To access a CIFS share on a NetApp core filer, there needs to be an export configured with a corresponding CIFS share.

1. Log in to the NetApp via telnet/ssh.
2. Verify that the export is configured to enable read/write and root access from the Avere client and cluster IP addresses. Verify using `exportfs -q /<VOLNAME>`
3. Export the volume and enable NFS root access for the volume.
   ```
   exportfs -p root=<NETWORK_IP/CIDR_SUBNET>,sec=sys,rw,anon=0,nosuid
   /<VOLNAME>
   ```
   Example: `exportfs -p root=10.0.0.0/8,sec=sys,rw,anon=0,nosuid /vol/cifsdemo`
4. Enable NTFS security style on the core filer volume.
   ```
   qtree security /<VOLNAME> ntfs
   ```
5. Create the CIFS share for the volume by using `cifs shares -add <SHARENAME> /<VOLNAME>`

6. Verify the Effective security style is NTFS with “Everyone” having “Full Control” of the root of the export. Example:

   ```
   fsecurity show /<VOLNAME>
   ```

   Example output (red font added for emphasis):

   ```
   [/vol/cifsdemo - Directory (inum 64)]
     Security style: NTFS
     Effective style: NTFS

     DOS attributes: 0x0030 (---AD---)

     Unix security:
         uid: 0 (root)
         gid: 0 (wheel)
         mode: 0777 (rwxrwxrwx)

     NTFS security descriptor:
         Owner: BUILTIN\Administrators
         Group: BUILTIN\Administrators
         DACL:
         Allow - Everyone - 0x001f01ff (Full Control)
         Allow - Everyone - 0x10000000 - OI|CI|IO
   ```

7. Avere OS utilizes NFSv3 for data path communications. To accomplish this, we require the UNIX root user to bypass ACL processing. We recommend isolating root access to Avere client cluster IPs and management hosts. Use export policies to restrict root user access to NTFS volumes that are exported via NFS. Use the global command `options cifs.nfs_root_ignore_acl on`
8. Map the root user to the Domain Administrator account, where <DOMAIN> is substituted with the real Active Directory domain name.

   Check if this mapping exists:

   ```
   rdfile /vol/vol0/etc/usermap.cfg
   ```

   To write the change to the file:

   ```
   wrfile -a /vol/vol0/etc/usermap.cfg "<DOMAIN>\Administrator == root"
   ```

9. Exit the telnet/ssh session using Ctrl D.

Steps to verify everything is working

Example NetApp commands to test LDAP configuration:

```
priv set advanced
getXXbyYY getpwbyname_r "AvereUser"
getXXbyYY getpwbyuid_r ${UID_ASSIGNED_TO_AVEREUSER}
getXXbyYY getgrbyname "Domain Users"
getXXbyYY getgrbygid ${GID_ASSIGNED_TO_DOMAIN_USERS}
wcc -u "AvereUser"
wcc -s "AvereUser"
cifs lookup "AvereUser"
cifs lookup "Domain Users"
```

note that the getXXbyYY command requires "priv set advanced" to be active.