Active Directory Administrator Guide to Avere FXT Deployment

Version 2014-07-16

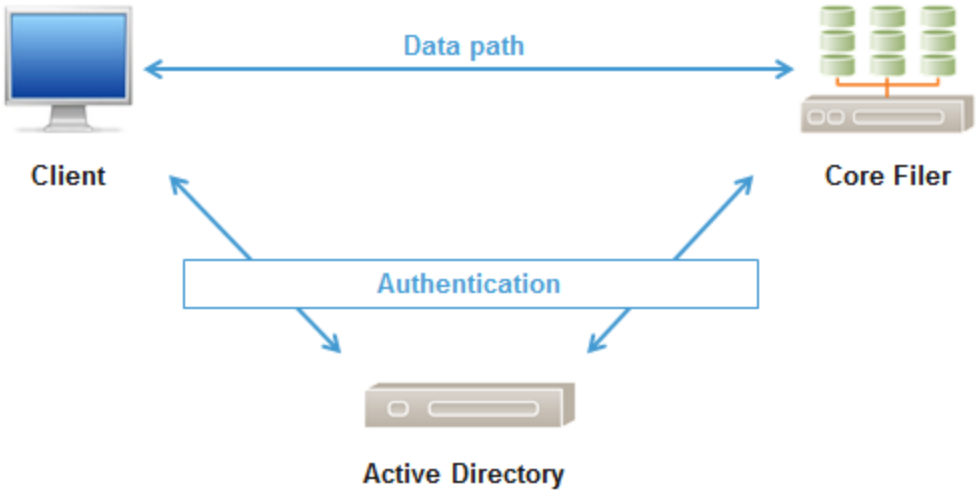
Copyright Information

Trademark Information

For licensing information on the third-party software used by the Avere product, see the Third-Party Licenses Reference.

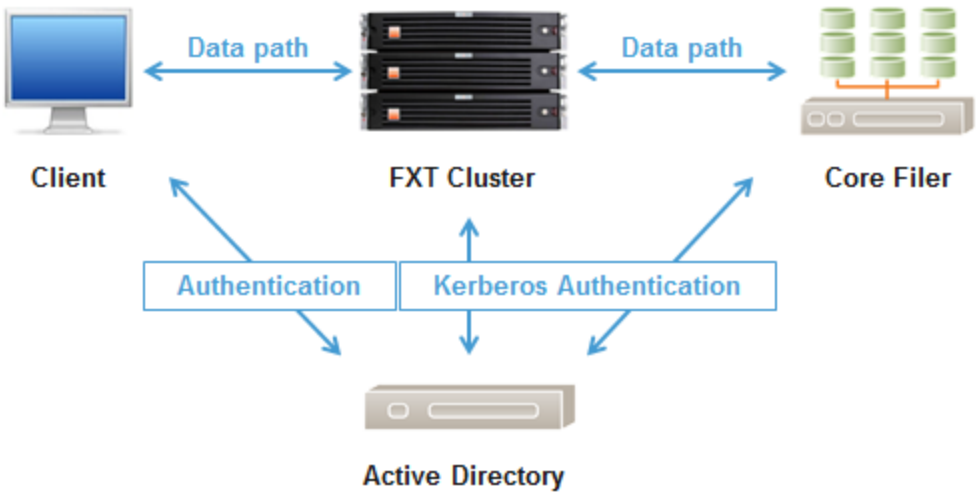
SUMMARY: FXT deployment requires a small amount of AD configuration. This configuration ensures continuous secure operation as the highly available FXT cluster is inserted into your environment.

Before Avere (NTFS Style Security)



Pre-Avere environment: clients access shares directly on core filers. All authentication is between clients and/or core filers within the Active Directory environment.

After Avere (NTFS Security Style)



Note: This assumes the customer is using NTFS security on their shares. If Posix mode bits are used (only), then much of the setup may be bypassed.

Each FXT CIFS-enabled VServer must make ACL requests to the core filer on behalf of authenticated clients' identities, and is enabled to do so via Kerberos configuration. This is known as delegation, and should be configured against only necessary services (CIFS) on the core filer, which is known as constrained delegation.

Constrained delegation gives administrators the ability to specify and enforce application trust boundaries by limiting the scope where application services on the FXT VServer can act on a user's behalf. This flexibility to constrain a service's authorization rights helps improve application security by reducing the opportunities for compromise by untrusted services.

These are mandatory configuration items for NTFS Security Style Shares.

ACTIVE DIRECTORY SETUP CHECKLIST

1. **Must be running Windows Server 2003 or later in Native Mode.**
2. **Machine Accounts for each FXT VServer** - Each VServer will require a machine account. An AD administrator with rights to add machine accounts, or an AD user account with sufficient permissions to add computers to the domain, is required. The machine account is placed in the '**Computers**' OU by default. Ensure this step is done during the addition of the machine accounts rather than trying to move them after creation.

   Adding VServers to another OU - This option requires a setting in the FXT GUI for "Organizational Unit" to be placed in an OU other than the default 'Computers'
3. **CLIENT ACCESS: VServer IP Addresses must be added as round-robin DNS (RRDNS) entries** - Each VServer has a range of IP addresses associated with it. These addresses are used for name resolution and SMB/CIFS share access. Each IP address must be added to the VServer hostname in DNS. This ensures round-robin resolution across all client-facing addresses. Refer to the Operations Guide, chapter 2 in the section labeled, "Setting DNS Parameters" for more information about using RRDNS.
4. **SPN / FQDN resolution** - The FXT cluster must be able to resolve the core filer DNS FQDN. Clients must be able to resolve the VServer FQDN consistently as well. If you are operating more than one DNS environment, both environments must resolve the names.

Core Filer Machine Account: Service Principal Name (SPN) The FXT vserver machine account must be able to request and obtain kerberos tickets for the CIFS service using the core filer FQDN server name (as configured in the FXT UI) as the kerberos principal. Therefore, the Core Filer Machine Account SPN name must match the fully qualified domain name.

5. **Domains** - The VServer machine and core filer machine accounts must be in the same Active Directory domain

6. **AD User/Group attributes** - The FXT cluster uses additional user and group attributes to process client requests. These are the UID and GID information. The attributes may be mapped to AD Users and Groups in two ways.

   - In Active Directory (recommended). You may configure each user/group who require access. Use ADSI Edit to modify.
   - In Flat File. You may enter mappings of Windows users to UIDs and GIDs, and store that file on the FXT Cluster.

How-To

1. Set SPN (Service Principal Name)

The Service Principal Name (SPN) allows Kerberos tickets to be obtained for the CIFS/SMB service on the core filer. A Service Principal Name must be configured for the core filer's CIFS Machine Account. This SPN is required for Kerberos constrained delegation.

To check if an SPN exists for CIFS, open a command prompt on the AD server and run `setspn -l <NetBIOS>` (example: `setspn -l netappsvr`) to list the service principals. If the SPN does not exist for CIFS and the FQDN, it must be added.

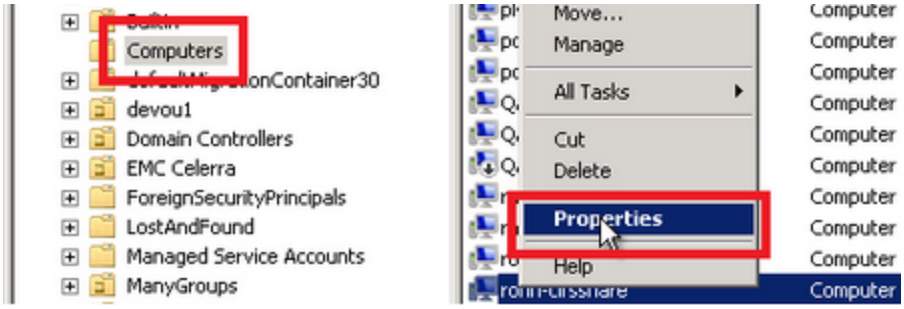
```
C:\Users\Administrator>setspn -l grapnel
Registered ServicePrincipalNames for CN=GRAPNEL,CN=Comp
        cifs/grapnel.dev.cc.arriad.com
        nfs/grapnel.dev.cc.arriad.com
        HOST/grapnel.dev.cc.arriad.com
```

To add a CIFS SPN, run: `setspn -A cifs/<core filer FQDN> <core filer NetBIOS>`

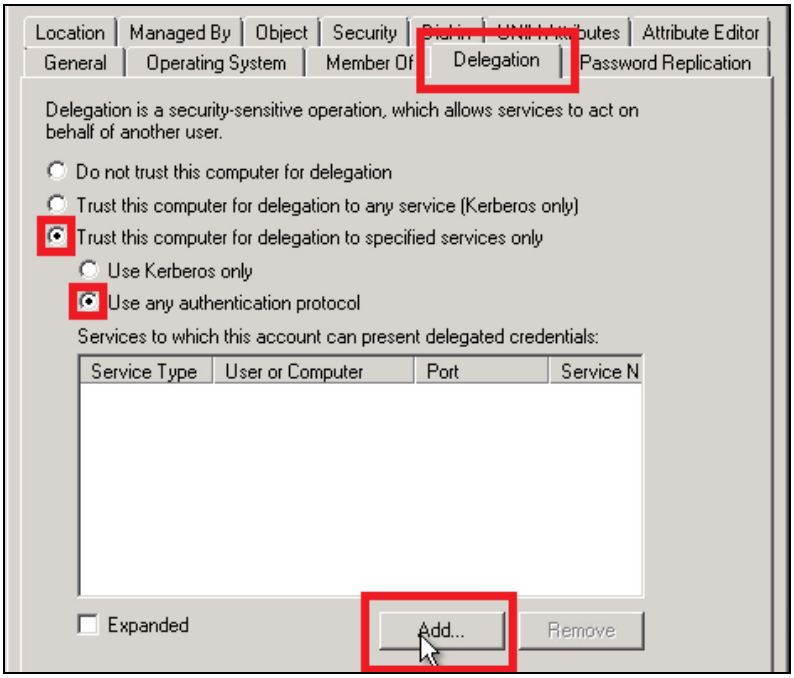
Example: `setspn -A cifs/netappsvr.arriad.com netappsvr`

2. Kerberos tickets via Constrained Delegation

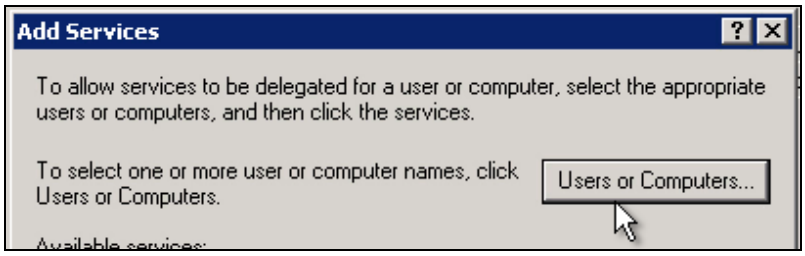
1. Open “Active Directory Users and Computers”.
2. Find the FXT VServer machine account in the OU that it was joined to (usually “Computers”).
3. Right click on the FXT VServer’s machine account object and select Properties.



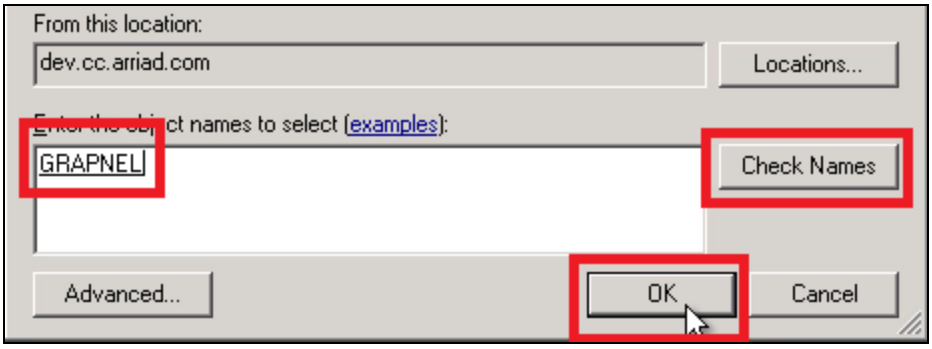
4. Select the Delegation tab.
5. Select "Trust this computer for delegation to specified services only.”
6. Select "Use any authentication protocol.”
7. Select Add.



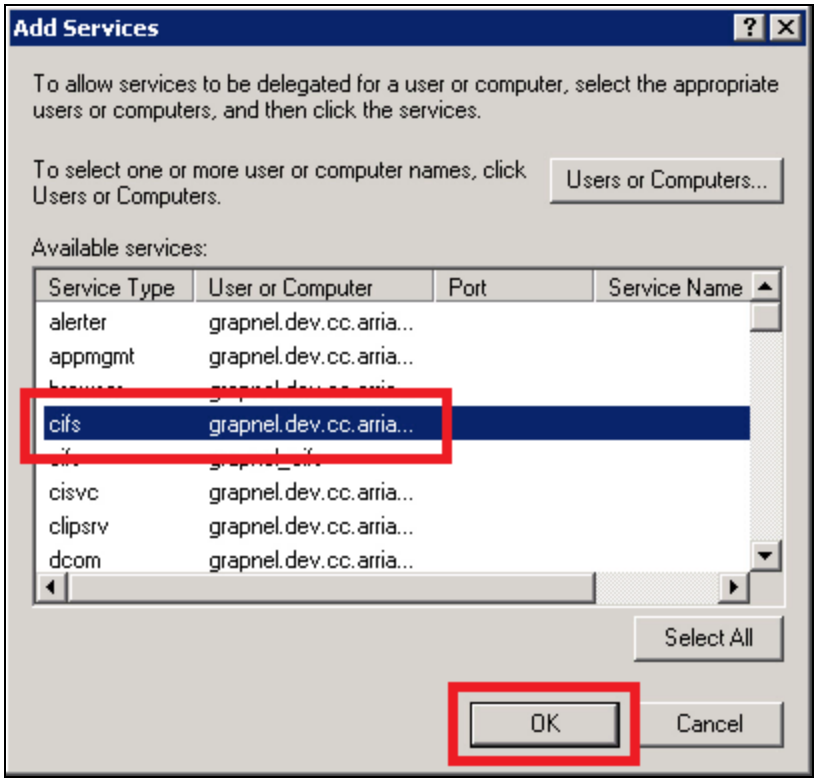
8. In the “Add Services” dialog, click the “Users or Computers” button.



9. Type the Core filer’s Machine Account.
10. Click the “Check Names” button.
11. When the core filer name is found, click OK.



12. Select the "CIFS" service type for the core filer’s machine account.
13. Click “OK”.



3. Assign User and Group Attributes with ADSI Edit

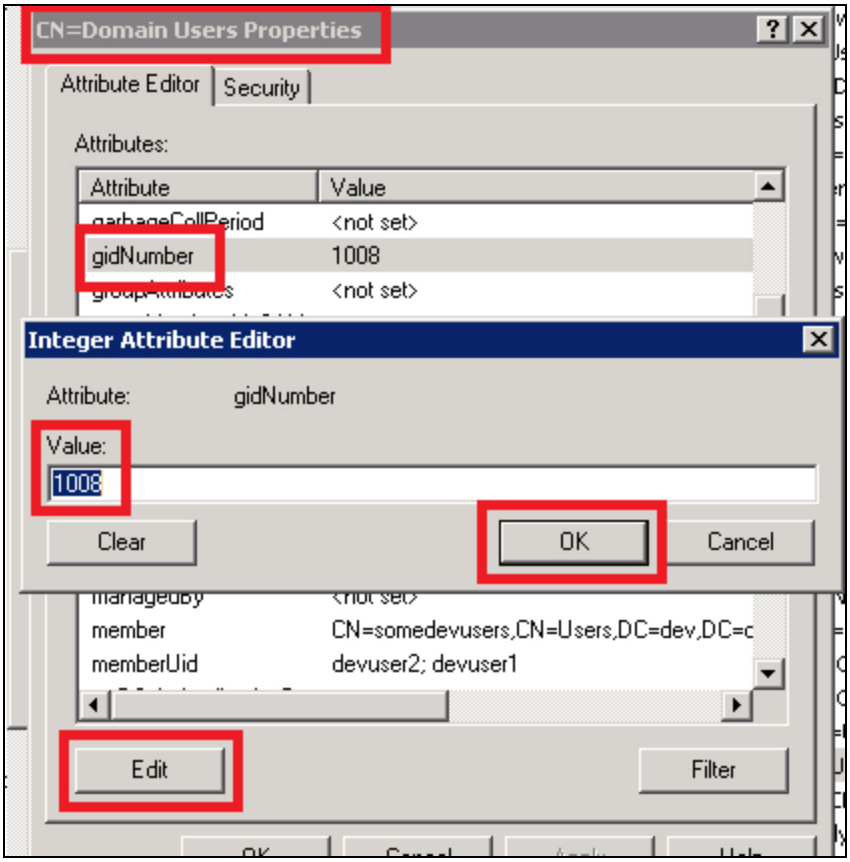
The Avere FXT cluster uses specific user attributes for NFS operations.

If your organization is using AD for LDAP:

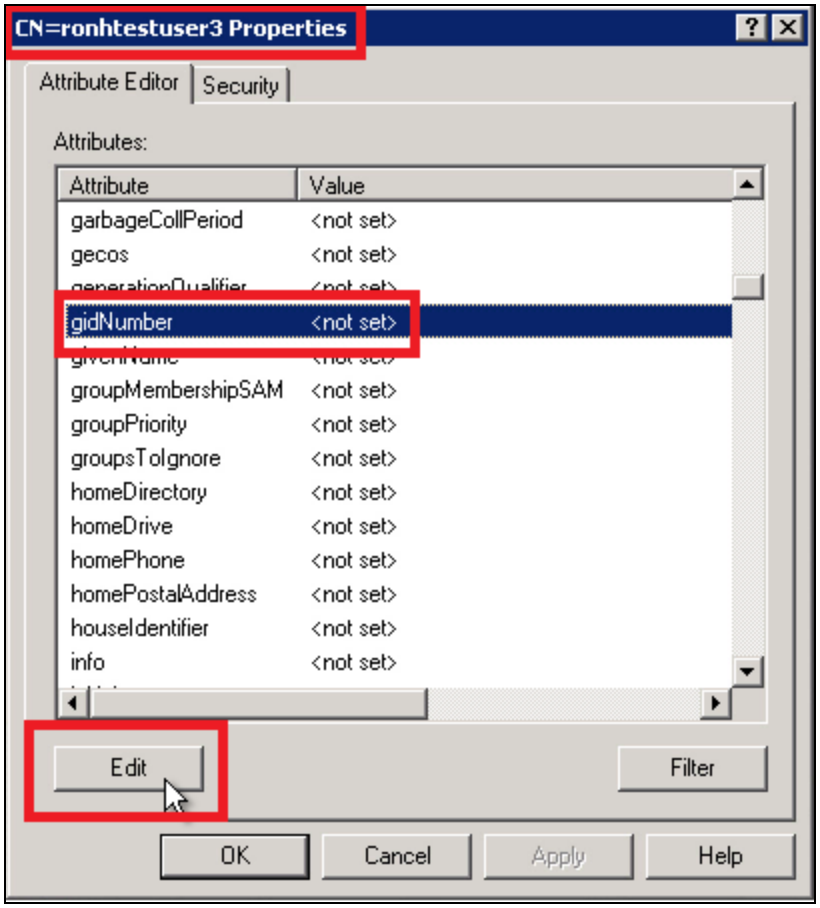
The easiest way to set the gidNumber and uidNumber attributes is to use ADSI Edit on the Active Directory server running adsiedit.msc.

A. Set the user's gidNumber attribute to match the "Domain Users" gidNumber.

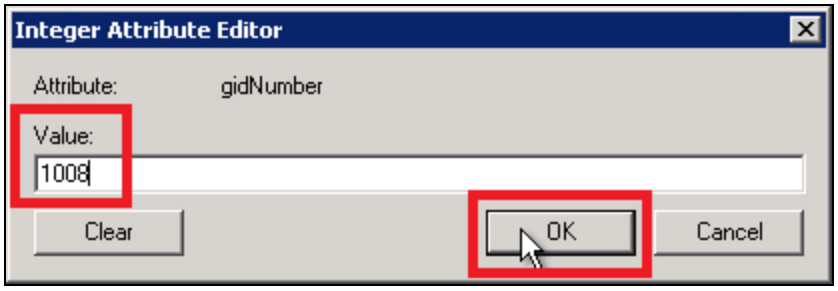
1. In ADSI Edit, right click CN=Domain Users & choose "Properties".
2. Find the attribute "gidNumber".
    a. If the value is "<not set>," we recommend setting it to a unique number between 10000 and 65000 by clicking Edit, clicking in the Value field, typing the number, and clicking OK. If the value is set, copy it.
3. Click OK and close the Domain Users Properties dialog box.



4. Right click the entry for the desired user and choose “Properties”.
5. Click the gidNumber attribute.
6. Click the Edit button.



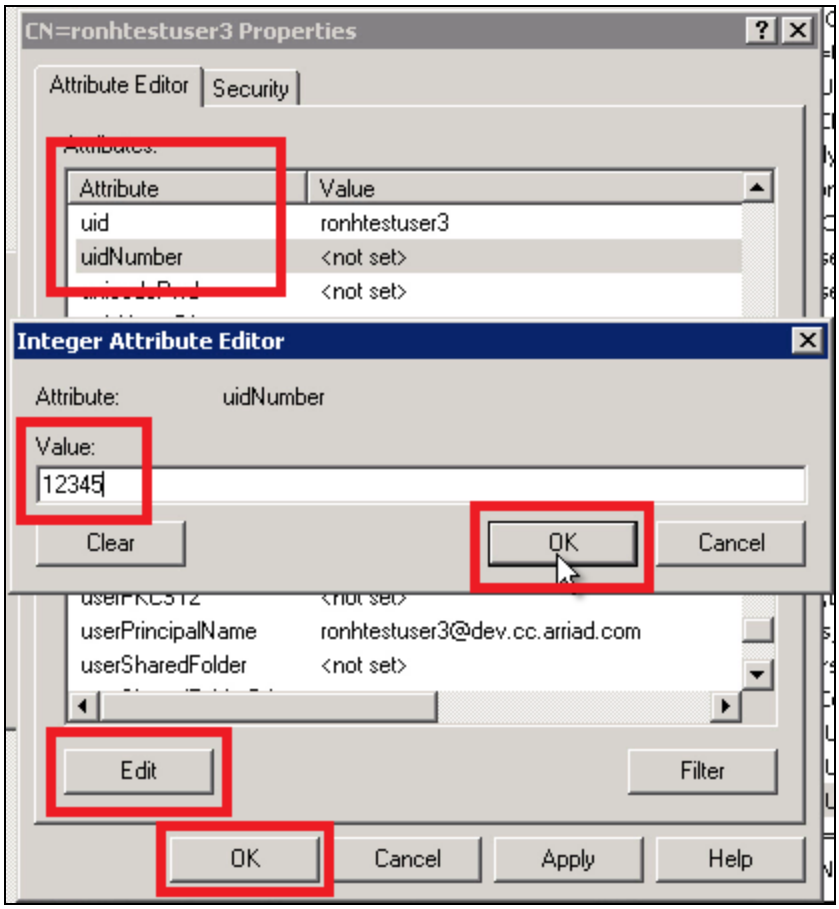
7. For the value, paste or type the gidNumber as taken from the gidNumber of “Domain Users” and then click OK.



B. Set the uidNumber attribute. Avere recommends a number between 10000 and 65000.

1. While in the ADSI Edit user properties, find and click the uidNumber attribute.
2. Click the Edit button.

3. Click in the Value field.
4. Enter a unique number between 10000 and 65000.
5. Click OK on the right.
6. Click OK on the bottom to commit attribute changes (gidNumber and uidNumber).



For SMB/CIFS client access, users are authenticated by their Windows credential but authorized based on their UNIX credential. This is required because the FXT uses NFSv3 for the datapath to the Core filer. For this reason, we require that users and groups have rfc2307 attributes in order to facilitate this.

A summary of required attributes are as follows:

User		
Attribute	**Description**	**FXT Use**
sAMAccountName	SMB username	Required. Automatically maintained by AD
uid	NFS username	If left blank (recommended,) defaults to sAMAaccountName
uidNumber	NFS userid	Required. Unique value must be assigned by admin
gidNumber	NFS primary groupid	Required. Value must be assigned by admin. Typically set to Domain Users gidNumber
Group		
cn	used as NFS groupname	Required. Automatically maintained by AD
gidNumber	NFS groupid	Required. Unique value must be assigned by admin
memberUid	member NFS usernames	optional for AD groups required for NFS groups when the core filer security style is posix mode bits and ad users are members of nfs groups

In order to successfully evaluate the entries on a core filer Access Control List (ACL), we need to be able to map a user and group Security ID (SID) to the corresponding UNIX credential.

To accomplish this, in addition to Active Directory for user authentication and SID-to-username translation, we also require a Directory Service as a source of these attributes. This can be NIS,

LDAP, or a flat file, whichever is the authoritative source of these attributes in your environment. If there are multiple sources, we should use the same source that the Core filer is using as it will also need to reverse translate from UNIX credential to Windows SID.

If there is not an authoritative source of these attributes, a flat file can be generated to provide these values. Alternatively, these can be populated in Active Directory via ADSIEdit. Active Directory can then be configured as the Directory Service via LDAP.\

The LDAP Server can be in a comma-separated list of servers. The BASE DN will match the LDAP DN of the domain.

Flat file format

User (/etc/passwd format)

i.e

<uid>:*:<uidNumber>:<gidNumber>:::

e.g.

avereuser:*:11111:10000:::

Group (/etc/group format)

i.e.

<cn>:*:<gidNumber>:<memberUid>,<memberUid>

e.g.

Domain Users:*:10000:avereuser,devuser1