Integrating NetApp Filers into Microsoft® Windows® Peer-to-Peer Workgroups

Paul Coartney | Network Appliance | March 2002 | TR-3148

TECHNICAL REPORT

Network Appliance, a pioneer and industry leader in data storage technology, helps organizations understand and meet complex technical challenges with advanced storage solutions and global data management strategies.

Table of Contents

1. Introduction

Microsoft Windows offers two security modes for authenticating users. These are domains and workgroups. Domains offer centralized authentication through domain controllers with a single common security database and are recommended for networks with more than a few machines. Workgroups require a security database of usernames and passwords be kept on each machine. Due to the burden of maintaining separate security databases, workgroups are only recommended for small installations. Network Appliance filers can be configured to run using domain or workgroup authentication. The aim of this paper is to detail the steps necessary to integrate a filer into a workgroup.

2. Methods of Authentication

In configuring the filer for workgroup mode, one has the choice of two methods of authenticating users. The first method discussed is based on developing and maintaining a UNIX® software-style password file on the filer. In heterogeneous environments, where both UNIX and Windows systems are used, this method can be implemented easily. In homogeneous Windows environments, creating and maintaining a UNIX style password file is cumbersome. To allow the filer to fit into these networks as seamlessly as possible, Network Appliance added an NT-style local security database beginning with Data ONTAP™ 6.1.

Which authentication scheme one chooses is dependent on the environment. Using the filer's security database is the easiest to implement, but has the limitation of supporting only 96 users (SAG 237).

3. Implementing UNIX Style Passwords

Whether one chooses to implement a UNIX style password file for compatibility with an existing UNIX network or because more than 96 user accounts are required, it will be necessary to do the following: enable clear-text passwords on each Windows host and create a password file on the filer. Table 3.1 matches the Microsoft® Knowledge Base article for enabling clear-text passwords with the corresponding operating system.

Operating System	Knowledge Base Article http://support.microsoft.com/
Windows 95, 98	No registry change required
Windows NT®	Q166730
Windows 2000	Q244627

Table 3.1. Knowledge Base articles for enabling clear-text passwords.

Once the Windows hosts are set for clear-text passwords, the remaining step is to create a password file on the filer. This can be accomplished in one of three ways: enabling the filer for NIS, copying a password file from an existing UNIX host to the filer, or manually creating one. Any of the three will allow for the use of UNIX passwords.

Probably the easiest of the three choices will be to add the filer as a NIS client into an existing NIS environment. Configuring the filer to run NIS is done by setting the NIS domain name, turning on NIS, and specifying how the filer will communicate with the NIS servers (CRG 147). Figure

3.1. illustrates these steps from the filer command line. Note: This task can also be accomplished from the FilerView® administrative user interface.

```
Filer> options nis.domainname domainname
Filer> options nis.enable on
Filer> options nis.servers ip_address, server_name, *

The arguments for nis.servers can be either a comma-delimited
list of IP addresses, hostnames, or an asterisk to bind in
broadcast mode.
```

Figure 3.1. Setting up NIS from the console.

If NIS is not in use but there are UNIX machines in the environment, it is possible to copy over the necessary files from a UNIX host to the filer. Since most recent versions of UNIX use "shadow" passwords where the encrypted passwords are kept in a file called /etc/shadow, it is necessary to copy over both the /etc/passwd and /etc/shadow files from the UNIX host to the filer. The filer will then look in the /etc/passwd file for usernames and in the /etc/shadow file for the corresponding encrypted password.

If neither NIS nor UNIX platforms exists in the environment, it is necessary to construct a password file and save it to /etc/passwd in the root volume of the filer. This can be done using the Windows WORDPAD utility as an editor. The UNIX password files consist of seven fields separated by colons; see figure 3.2. The fields are as follows:

Username - maximum of eight characters
Encrypted Password - thirteen characters; by default they are blank on the filer
UID - user ID, unique number between 0 and 65535; 0 is reserved for the root user
GID - group ID; user's primary UNIX group corresponds to the group number in /etc/group, also 0 through 65535
GECOS - description of the account, usually the user's full name
Login Directory - usually user's home directory
Shell - default shell for login

```
root::0:1::/:
pcuser::65534:65534::/:
nobody::65535:65535::/:
```

Figure 3.2. Default password file, /etc/passwd, from the filer.

The filer will only use the first four fields. The password is sent to the filer in clear-text and is encrypted by the filer using the same salt as the saved encrypted password. If the two encrypted passwords match, access is granted. If no password is included in the encrypted password field, access is denied. Unlike UNIX, access will not be granted with a blank password.

The filer may already have an /etc/passwd file, similar to the one in figure 3.2, in the root volume that contains entries for root, pcuser, and nobody. If it does, open the file with WORDPAD and add an entry for each new user. If no /etc/passwd file exists on the root volume, create one with WORDPAD. It is important to use WORDPAD and not NOTEPAD due to the differences in characters between Windows and UNIX. To generate an encrypted password, go to the

command line on the filer and change to advanced mode with the priv set advanced command. The cifs passwd command can be used to generate the encrypted passwords as shown in figure 3.3.

```
Filer> priv set advanced
Filer*> cifs passwd yellow (The * denotes advanced mode.)
Filer*> password is aslyrvh.Ddw3e
Filer*> priv set admin
Filer>
```

Figure 3.3. Encrypting the password *yellow* on the filer.

The encrypted password is returned. So, if we are adding the user John Jones whose username is *jones* with password *yellow*, UID *1000*, and GID *100*, the entry becomes:

jones:aslyrvh.Ddw3e:1000:100:John Jones::

It is important the UIDs do not get reused and are unique. Usernames and passwords are case sensitive. In all but the simplest environments this can be tedious to set up and maintain. When a user changes his or her Windows password, the filer's password will not be changed. If this doesn't work after the initial setup, chances are clear-text passwords have not been enabled properly; it is necessary to reboot the Windows machine after changing registry settings. If users encounter problems, it is most likely due to using the wrong password (users trying their Window's password and not the filer's password).

4. Implementing Local Users with useradmin

An alternate method for maintaining users' accounts for filers running Data ONTAP 6.1 or later is by using the useradmin utility to add users to the local accounts database. The man page for useradmin can be found on page 224 of the *Data ONTAP Command Reference Guide*. By default there is a built-in administrator account; see figure 4.1. Adding local users to the filer is accomplished from the filer console command line as illustrated in figure 4.2. Here again we are adding the user John Jones with username jones and password *yellow*. Note that the password must be at least six characters in length. Once this is done, the user should be able to map a drive and use the filer to store and retrieve files. This is by far the easiest method to use and maintain local user accounts in a homogeneous Windows environment.

```
Filer> useradmin userlist
List of all non-root users:
Name: administrator
Console Login Allowed: no
Info: Built-in account for administering the filer
Full Name:
Rid: 500
```

Figure 4.1. Default local user database entries.

```
Filer> useradmin useradd -c "Jim Jones" jones
Filer> New Password:
Filer> Retype new password:
Filer> User added.
```

```
Filer> useradmin userlist
Filer> List of all non-root users:
Name: administrator
Console Login Allowed: no
Info: Built-in account for administering the filer
Full Name:
Rid: 500

Name: jones
Console Login Allowed: yes
Info: Jim Jones
Full Name:
Rid: 131073
```

Figure 4.2. Using useradmin to add users to the local database.

5. Mapping a Drive

Once a method of authentication is set up, mapping a drive is done in the same manner as it would be for mapping a drive from any Windows file server. Of course, the exact details of each change depend on the version of Windows being used. Windows 95 and 98 do not provide a way to specify an alternate username when mapping a drive, so the Window's username and filer's username must match.

To map the drive, right click Network Neighborhood and choose Map Network Drive from the selections. For Windows 95 and 98, the username and password supplied at login must match the filer's username and login. For Windows NT, one should enter *filername**username* in the Connect As field and then supply the password for your account on the filer when prompted. For Windows 2000, use the Connect as a Different User under the Map Network Drive option and specify *filername**username* for username and the user's password for the filer.

6. Summary

The filer is capable of participating in either Microsoft Windows domain or workgroup authentication models. As is the case in all PC workgroups, setting up and maintaining the workgroup mode is more tedious for the administrator. Network Appliance has worked to make this easier by adding local user accounts in Data ONTAP 6.1.

7. References

Data ONTAP System Administrator's Guide, March 2001, Network Appliance, Sunnyvale CA. (SAG)

Data ONTAP Command Reference Guide, March 2001, Network Appliance, Sunnyvale, CA. (CRG)

NetApp®

Network Appliance, Inc.
495 East Java Drive
Sunnyvale, CA 94089
www.netapp.com