How Network Appliance™ Devices Join Active Directory: Covering Data ONTAP™ 7.0 RC1 for NetApp filers, qFiler™, and NearStore® and Data ONTAP 6.0 RC1 for NetCache®

by Bill Katz and Peter Henneberry,

Network Appliance, Inc.

December, 2004 | TR 3362

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. Objectives

This document explains the basic methods used to join a Network Appliance device to a Microsoft® Active Directory (AD) domain and the rights required to do so.

2. Why Is Joining a NetApp Device to Active Directory Necessary?

In order for resources on a network to be locatable, a mechanism must exist whereby the resources can easily be found. A directory service—in this case, AD—keeps track of all known resources and responds to requests with a list of currently available devices and services. But before you can be trusted to query for resources, you must be granted membership in the Active Directory domain.

The key benefits for a NetApp device to join Active Directory are:

- Controlled security and management through group management—i.e., group policy objects (GPOs) and access control lists (ACLs) placed on objects and organization units (OUs)
- Single-sign-on and pass-through authentication for users
- Interoperability by extending control beyond the native Windows® environment through the Microsoft management interface by providing a read-only computer management view of:
    - Shared folders, shares, sessions, and open files
    - Local users and groups to the NetApp device

2.1. Machines Need Accounts Too

Every computer running a Windows workstation (Windows NT 4.0 or higher), Windows server operating system, or NetApp device has a computer account. As for users, who require a valid account before being allowed to access a networked resource, so too is it requisite that workstations, servers, and other devices participating in an Active Directory domain have an account, which provides a means for authenticating and auditing computer access to the network and access control, security, and management to domain resources.

2.2. Active Directory Join Methodology

Active Directory provides two methods for an AD device-aware object to join Active Directory.

- First precreate the computer object using an account with the required privileges, and later use an account with fewer privileges to log on to the computer and issue the appropriate command to complete the join process.

- Or, use an administrator equivalent account during the Active Directory join process.

Data ONTAP is a proprietary operating system developed by Network Appliance; it is not based on the Windows OS. Consequently, the current Data ONTAP operating system requires additional rights assigned to the user or to the precreated device object when an administrator or administrator equivalent account is not used. Once the computer object has successfully joined the Active Directory domain, the user account credentials will no longer be used and are not stored in any way in the OS. They are used only to allow the NetApp device to become an active member of AD and to write standard properties to the object during the join process (the properties that are written are listed in the next section).

2.3. Joining a NetApp Device to Active Directory

2.3.1. Method 1: Precreating a Computer Object

(This is the method recommended by NetApp.) Many Active Directory administrators employ a set of best practices that place strict controls over who can create computer objects. If the join is performed in the following manner, security risks are minimized because the need for Active Directory admin rights at the device during the setup process is eliminated.

1. A new computer object for the NetApp device is created in AD. The computer object should be placed in the container (i.e., domain, organizational unit, computer) most appropriate for the organizational structure of your AD layout.

2. Assign the following two rights to one of the following:

   a. The AD container where the computer object was added

   b. The computer object

   c. The user who will complete the join process

      Change Password (or Reset Password). This allows changing the default password.
      Write Public Information. This is required for version information.

   NOTE: Selecting option 2b, the computer object, to add the two additional rights requires more administrative work, since each computer account for each NetApp device would need to be modified.

   A user account with minimum rights may be utilized when the NetApp object is precreated before the join process is executed. At the completion of the AD join process, a number of properties are written to the computer account, including:

   - DNS host name

   - Several service principal names

- Object classes
- Operating system name and version
- A randomly generated password is set for this account via KPASSWD (Note: This is the only instance in which the NetApp join process differs from the Microsoft join process. Microsoft uses proprietary RPC calls to change the password, whereas NetApp uses the published KPASSWD APIs to accomplish this task.)

2.3.2. Method 2: Account with Rights to Join Computer Object to Active Directory

This section describes how a NetApp device joins Active Directory using a domain administrator's account or equivalent to create the Active Directory computer object. Because of this, Network Appliance only recommends this approach for organizations that do not need or employ more restrictive access policies.

1. Choose one of the following account types to use:
   - An administrator or administrator equivalent account
   - A standard user account, which needs to have the Change Password (or Reset Password), Write Public Information, and Create Computer Objects rights; this allows creation of the NetApp object
   - The organization unit where the NetApp device will be added, with the following three rights:
     a. Change Password (or Reset Password)
     b. Write Public Information
     c. Create Computer Objects
2. Use a standard user account for the AD join process.

   NOTE: This option is strongly discouraged for security reasons, because it allows any user to create a computer account in the specified context.

3. Conclusion

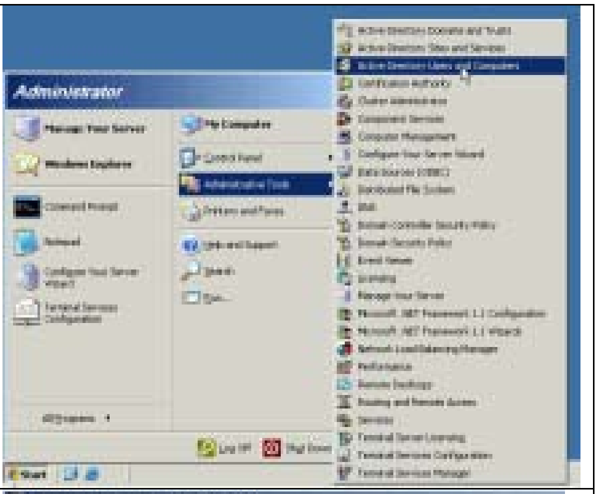
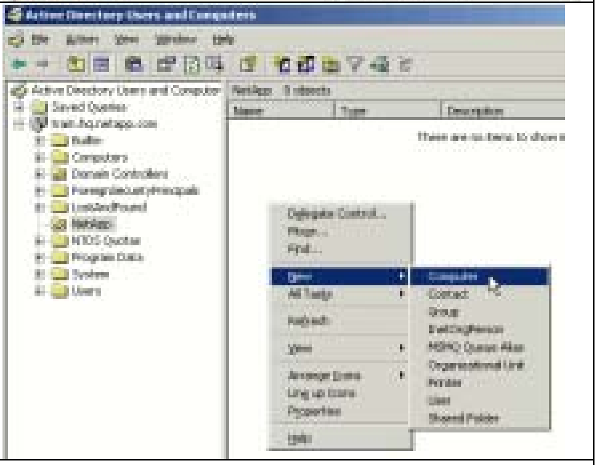
To locate resources on a network, a mechanism must exist whereby the resources can easily be found. A directory service—in this case, AD—keeps track of all known resources and responds to requests with a list of currently available devices and services. But before you can be trusted to query for resources, you must be granted membership in the domain.

Joining a domain accomplishes two tasks. First, for a NetApp device, it grants the required rights to query AD, should it need to find other resources. Second, it provides a single management interface through MMC for administration of security and users' access levels to the NetApp device.

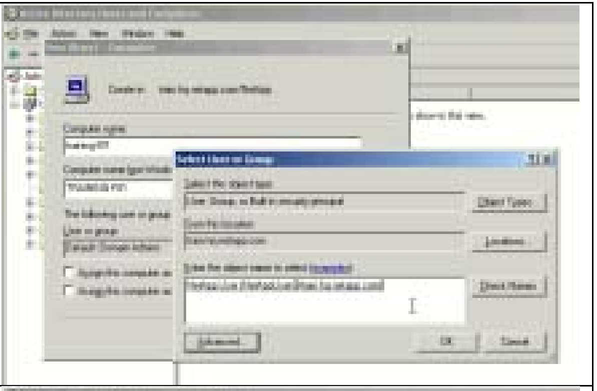
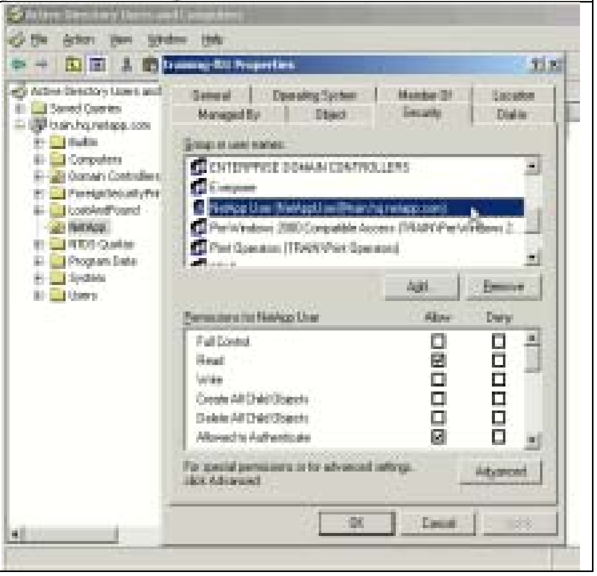
4. Appendices

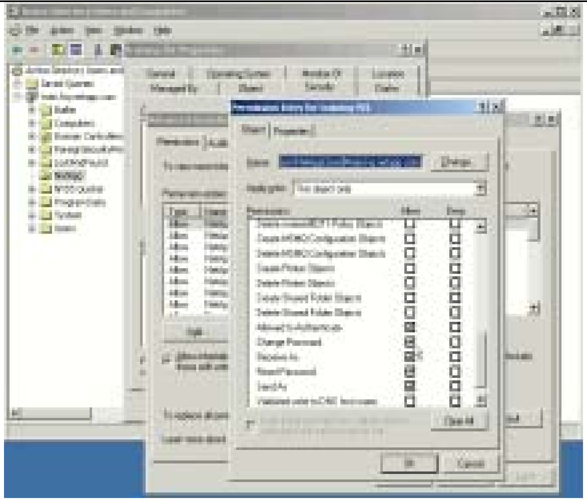
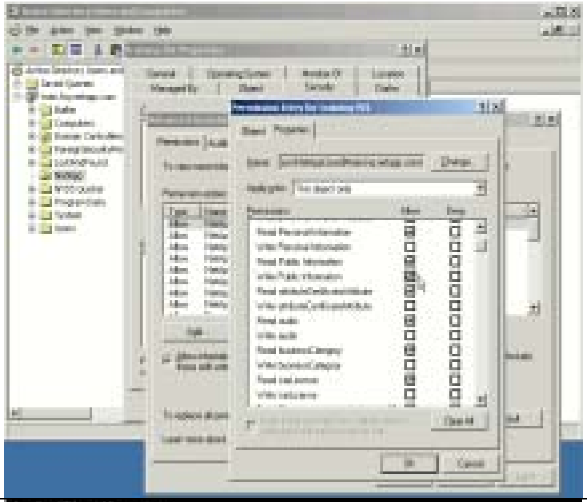
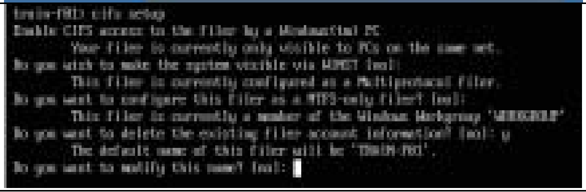
4.1. Appendix A: Detailed Restricted User Account Join Procedure

The following steps describe how to join the domain using the procedure described in Section 2.3 as "Method 1, 2b": i.e., precreation of a computer object account, with minimal privileges being assigned to a specific user to join the computer to the domain.

1	Using Microsoft Management Console (MMC), open “Active Directory Users and Computers.” On the View menu, ensure that Advanced Features is checked.	
2	In the Active Directory tree, select the organizational unit for the NetApp device, right-click, and choose New > Computer.	
3	Enter the device’s (computer object’s) name. A NetApp device supports up to 64 characters for the computer object name.	

Administrator
Manage Your Server
Windows Explorer
Command Prompt
Notepad
Configure Your Server Wizard
Terminal Services Configuration
All Programs
My Computer
Control Panel
Administrative Tools
Printers and Faxes
Help and Support
Search
Run...
Log Off
Shut Down
Start
Active Directory Domains and Trusts
Active Directory Sites and Services
Active Directory Users and Computers
Certification Authority
Cluster Administrator
Component Services
Computer Management
Configure Your Server Wizard
Data Sources (ODBC)
Distributed File System
DNS
Domain Controller Security Policy
Domain Security Policy
Event Viewer
Licensing
Manage Your Server
Microsoft .NET Framework 1.1 Configuration
Microsoft .NET Framework 1.1 Wizards
Network Load Balancing Manager
Performance
Remote Desktop
Routing and Remote Access
Services
Terminal Server Licensing
Terminal Services Configuration
Terminal Services Manager

4	In “The following user or group can join this computer to a domain,” specify the user account you will later use to join the NetApp device to Active Directory. Click Next to complete the creation of the computer object.	
5	Right-click the computer object and choose Properties. Click the Security tab.	 Group or user names: ENTERPRISE DOMAIN CONTROLLERS Everyone NetApp User (NetAppUser@train.hq.netapp.com) Pre-Windows 2000 Compatible Access (TRAIN\Pre-Windows 2... Print Operators (TRAIN\Print Operators) Permissions for NetApp User — Allow / Deny Full Control □ □ Read ☑ □ Write □ □ Create All Child Objects □ □ Delete All Child Objects □ □ Allowed to Authenticate ☑ □ For special permissions or for advanced settings, click Advanced.
6	Select the user that you will use to add the device to the Active Directory domain.	

7	In "Permissions for <Group or user name selected>," click Advanced. Select the user created in step 6 and click Edit. In addition to the default user rights, enable the following two rights: • On the Object tab, allow Change Password (or Reset Password) • On the Properties tab, allow Write Public Information	 
8	Run the CIFS configuration on the NetApp device. At the prompt "Please enter the new hostname," enter the device name exactly as you specified it in step 3.	 train-FAS1> cifs setup Enable CIFS access to the filer by a Windows(tm) PC Your filer is currently only visible to PCs on the same net. Do you wish to make the system visible via WINS? [no]: This filer is currently configured as a Multiprotocol filer. Do you want to configure this filer as a NTFS-only filer? [no]: This filer is currently a member of the Windows Workgroup 'WORKGROUP' Do you want to delete the existing filer account information? [no]: y The default name of this filer will be 'TRAIN-FAS1'. Do you want to modify this name? [no]:
9	At the "Please enter the Windows 2000 user [Administrator@<domainname>]:" prompt, do not press Enter. Instead, type the name of your user account from step 6. When prompted, enter the user account's password.	

4.2. Appendix B: Should Active Directory Be in Mixed or Native Mode?

The terms **mixed mode** and **native mode** refer to functional levels in a Windows 2000 server. In a Windows 2003 server, the terms mixed and native have been superseded by **Raise Function Level**.

Domain Function Levels (Mixed and Native)

There are now four domain levels in which a Windows 2003 server can operate.

- **Windows 2003 server.** All Windows 2003 servers, no other domain controllers. However, even in this level, the whole range of clients (including NetApp devices) and member servers can still join the domain.

- **Windows 2003 server interim.** Windows NT® 4.0 servers and Window 2003 servers (no Windows 2000). This level arises when you upgrade a Windows NT 4.0 PDC to a Windows 2003 server. Interim mode is important when you have Windows NT 4.0 groups with more than 5000 members. Windows 2000 does not allow you to create groups with more than 5000 members.

- **Windows 2000 native.** Allows Windows 2000 and Windows 2003 servers (no Windows NT 4.0).

- **Windows 2000 mixed.** Allows Windows NT 4.0 BDCs and Windows 2000. Naturally Windows 2000 mixed is the default function level, because it supports all types of domain controllers.

NetApp Devices

A NetApp device may be joined to Active Directory whether in mixed, native, interim, or pure Windows 2003 server mode.

4.3. Appendix C: Troubleshooting the Domain-Joining Process

DNS. In order to determine whether the NetApp device is joining a Windows NT 4.0 domain or Active Directory and to locate domain controllers, a key distribution center (KDC used for Kerberos), and other necessary services, CIFS relies on DNS. If DNS is not enabled or is configured incorrectly, the domain-joining phase will either fail or, if a Microsoft Windows Internet-naming server (WINS) is running, assume that the domain being joined is a Windows NT 4.0 domain.

Time synchronization. If time synchronization is not enabled, and the NetApp device's time drifts by more than five minutes from the domain's time, client authentication attempts to the NetApp device will fail until corrected.

Active Directory replication. Based on the size of the Active Directory domain, to propagate a change for a small organization with one site, the replication will usually take less than 15 minutes. For a global company with many sites, the replication may take up to several hours to complete.

4.4. Appendix D: Device Discovery

The NetApp device performs an intelligent discovery process to locate the most appropriate domain controller (DC) in the network with which to communicate. For its first connection, Data ONTAP attempts to use servers that appear in the CIFS prefdc list (in list order), if configured. If none of these preferred servers is available, or if none is configured, all server addresses are discovered at once, then categorized, prioritized, and cached.

Preferred addresses are ordered as specified using the cifs prefdc command. "Favored" and "other" categories are sorted according to the fastest response. Data ONTAP simultaneously pings all addresses listed in both categories and waits one second for responses.

The cifs prefdc command allows control over the order in which Data ONTAP attempts contacting a server. The list is consulted for all Windows service connections, not just domain controllers.

When configuring CIFS on a NetApp device in a Windows 2000/2003 domain, an LDAP query to AD checks to ensure a computer object with the same name doesn't already exist. If the name does exist, the setup process makes sure it is not a domain controller. These are precautionary measures used to guarantee no computer object names are duplicated in error.

4.5. Appendix E: Reference Material

The following resources provide additional information on Microsoft Active Directory and joining a computer object.

Microsoft Knowledge Base

- Domain Users Cannot Join Workstation or Server to a Domain
- Enhanced Security Joining or Resetting Machine Account in Windows 2000 Domain
- Time Synchronization

What Is Microsoft Active Directory?

- Windows 2000 Advanced Server Documentation

Third-Party References

- Precreating Computer Objects to Join Active Directory
- Understanding Active Directory
- Active Directory "Cookbook"