Technical Report

NetApp Storage Systems in a Microsoft Windows Environment

Reena Gupta, NetApp; updated by Bingxue Cai, NetApp
April 2011 | TR-3367

INTEGRATION WITH MICROSOFT WINDOWS

File services are an essential part of every customer's storage environment. NetApp® storage systems deliver highly reliable file services to Microsoft® Windows® clients using the Common Internet File System (CIFS) protocol. This document describes how storage systems work seamlessly in the Microsoft Windows environment and all the features related to Microsoft Windows that are supported by NetApp systems. Beginning with Data ONTAP® 7.3.1, NetApp storage systems also support SMB 2.0 protocol for Windows file serving.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1 PURPOSE AND SCOPE

NetApp storage systems deliver highly reliable file services to Microsoft Windows clients by using the Common Internet File System (CIFS) protocol. This document describes how our storage systems work seamlessly in the Microsoft Windows environment and how they enable you to effortlessly manage data by making use of standard Microsoft services and features such as Active Directory®, IntelliMirror, Volume Shadow Copy, Access-Based Enumeration, Offline File Caching, Auditing, Distributed File System (DFS), File Screening, and CIFS Virus Protection.

This document provides a high-level view of how NetApp storage systems integrate in Microsoft Windows environments. Specifically, this document discusses the following topics:

- How storage systems can be integrated in mixed-mode or native-mode Active Directory environments and different authentication types
- How administrative tools based on Windows, such as the Microsoft Management Console of Active Directory Users and Computers, can be used to perform Windows administration tasks on a NetApp storage system
- How Data ONTAP supports security in a Windows environment such as NTLMv2, Server Message Block (SMB) signing, LDAP signing, virus scanning, and file screening
- How Data ONTAP supports Windows client-side features that are typically used in most Windows environments
- How Data ONTAP facilitates home directory deployments

For procedural information about using these features and services on NetApp storage systems with Windows servers, refer to the "Data ONTAP File Access and Protocol Management Guide," available from the NetApp Support (formerly NOW™) site at http://now.netapp.com.

This document covers the features related to the Windows environment that are supported in Data ONTAP 8.0 7-Mode; it does not cover Data ONTAP GX. To check the compatibility and support matrix for different Windows operating systems, refer to the Windows File Service Compatibility Matrix on the NetApp Support site.

For detailed information about the Microsoft services and features discussed in this paper, refer to www.microsoft.com.

2 ASSUMPTIONS

To benefit from this report, NetApp assumes that the reader is familiar with:

- Microsoft Windows 2000 Server, Windows Server 2003 (R2), Windows Server 2008, Windows Vista®, and Windows XP® products and their features
- NetApp storage system administration; for information about storage system administration, refer to the Data ONTAP administration guides available at http://now.netapp.com

3 INTRODUCTION

NetApp storage systems are storage appliances powered by NetApp Data ONTAP software. Data ONTAP optimizes file service by combining the WAFL® (Write Anywhere File Layout) file system and a microkernel design dedicated to network data access.

NetApp systems are compatible with Microsoft Windows environments, whether operating as network-attached storage (NAS), as a storage area network (SAN), or both. In Windows file-serving environments, storage systems look and act like Microsoft Windows member servers and can be monitored and administered using native Windows management components while providing highly available file service.

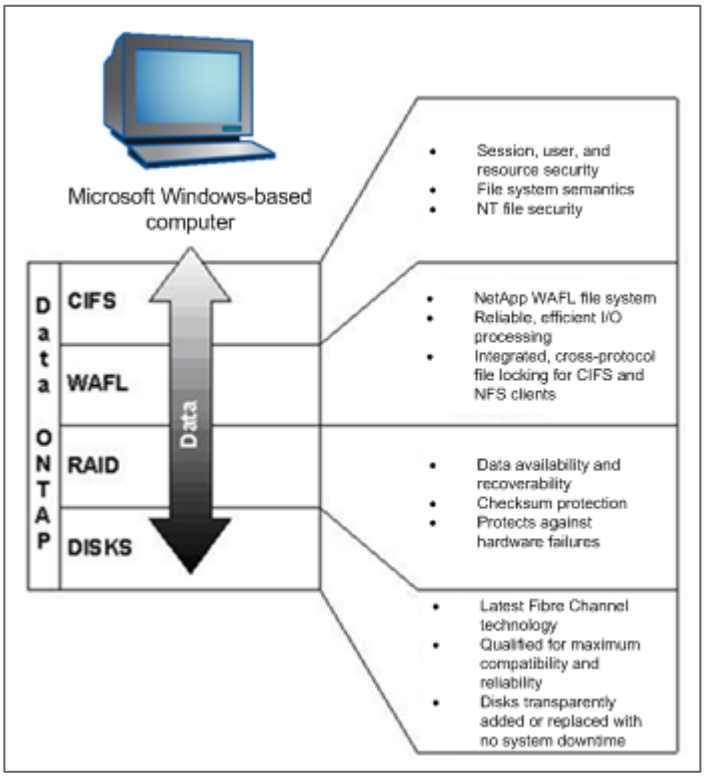
NetApp systems use the Microsoft industry-standard CIFS/SMB protocol and support native implementations of the Lightweight Directory Access Protocol (LDAP) and the Kerberos authentication protocol without requiring additional software.

4 INTERACTION BETWEEN NETAPP AND WINDOWS SYSTEMS

The CIFS protocol is natively integrated into Data ONTAP. As a result, Windows 2000, Windows XP, Windows 2003, Windows Vista, and Windows 2008 computers do not require additional client software to access data on NetApp systems. Storage systems appear on the network as native file servers.

Figure 1 depicts the file input/output (I/O) path between Windows computers and the storage systems.

Figure 1) Windows computers and storage system I/O path.



Just as a database uses a transaction log, the WAFL on-disk file system uses nonvolatile random access memory (NVRAM). This log-structured approach maximizes reliability and makes sure that the file system is always consistent. NetApp Snapshot® technology leverages WAFL consistency points to create near-instantaneous online volume backups. This allows end users to recover their own deleted or modified files using either Microsoft shadow copies of shared folders or simple drag-and-drop methods in Windows Explorer. NetApp SnapRestore® technology makes it possible to recover very large databases from online backups in minutes rather than hours. Snapshot copies are easily managed, require minimal disk space, and are easily accessed.

5 SMB 2.0 PROTOCOL SUPPORT

Beginning with Data ONTAP 7.3.1, NetApp storage systems support SMB 2.0, the next-generation CIFS protocol, in coexistence with the CIFS/SMB protocol. SMB 2.0 is a complete redesign of the previous CIFS/SMB protocol. SMB 2.0 protocol has the following features:

- Compounded operations
- Durable handles
- Credit system
- Large buffer, up to 64K
- SMB signing
- Increased scalability

All of these SMB 2.0 features corelate to certain advantages over the CIFS/SMB protocol, as listed in Table 1.

Table 1) SMB 2.0 features and benefits.

Benefit	Features	What It Means to Customers
Enhanced performance	• Compounding operations • Larger buffer size • Crediting (QoS)	• Large reads and writes in fewer round trips with 64KB buffer size • Improved WAN performance • Server can do some load balancing with credit granting
Increased server scalability	• Extended session ID and tree ID fields • Extended UID and FID namespace	• Up to 128K number of user sessions and tree connections per TCP connection
Network resiliency and increased reliability	• Asynchronous messages • Durable handles	• Fewer timeouts on the CIFS sessions • Avoids data loss on the client side
Enhanced security	• SMB signing using SHA256	• More robust “secured signing algorithm”

SMB 2.0 can be enabled in Data ONTAP 8.0 using the option `cifs.smb2.enable`; it’s disabled by default. For additional details on SMB 2.0 implementation in Data ONTAP, refer to TR-3740: SMB 2.0– Next-Generation CIFS Protocol in Data ONTAP.

6 ACTIVE DIRECTORY SUPPORT

The Microsoft Active Directory service allows organizations to efficiently organize, manage, and control resources. Active Directory is implemented as a distributed, scalable database managed by Windows 2008, Windows 2003 (R2), or Windows 2000 domain controllers.

Functional levels determine the available Active Directory Domain Services (AD DS) domain or forest capabilities. They also determine which Windows Server operating systems you can run on domain controllers in the domain or forest. However, functional levels do not affect which operating systems you can run on workstations and member servers that are joined to the domain or forest. Active Directory has two types of functional levels: the domain and the forest.

DOMAIN FUNCTIONAL LEVELS

Domain functionality activates features that affect the whole domain and one of the following domains only. These levels are distinguished by the version of the Windows Server operating system that is

permitted on the domain controllers present in the domain. With each successive level increase, the domain functionality activates features of the previous domain level.

FOREST FUNCTIONAL LEVELS

Forest functionality activates features across all the domains in your forest.

NetApp storage systems can join and participate in the domain/forest functional levels of Active Directory shown in Table 2.

Table 2) Domain and forest functional levels.

Domain/Forest Functional Level	Supported Domain Controllers
Windows 2000 mixed	Windows NT® 4.0 Windows 2000
Windows 2000 native	Windows 2000 Windows Server 2003 Windows Server 2008 Windows Server 2008R2
Windows Server 2003	Windows Server 2003 Windows Server 2008 Windows Server 2008R2
Windows Server 2008	Windows Server 2008 Windows Server 2008R2
Windows Server 2008R2	Windows Server 2008R2

Note: For details on the enabled features for each of these functional levels, refer to the Microsoft Web site.

NetApp storage systems can also participate in a multidomain infrastructure in which it can join one domain and other domains have trust relationships with this domain.

6.1 NAME RESOLUTION

Similar to Windows 2000, Windows 2003 (R2), and Windows 2008 computers in an Active Directory environment, NetApp storage systems query Domain Name Service (DNS) servers to locate domain controllers. The Active Directory service relies on DNS to resolve names and services to IP addresses; therefore, the DNS servers that are used with storage systems in an Active Directory environment must support service location (SRV) resource records (per RFC 2782). If the DNS is not enabled or is not configured correctly, Data ONTAP will not be able to find the service records it needs to locate the DCs, KDCs, LDAP servers, and KPASSWD servers, and it will not be able to join the Active Directory domain.

Note: Microsoft recommends DNS servers that support dynamic updates (per RFC 2136) so that important changes to SRV records about domain controllers are automatically updated and immediately available to clients. Beginning with Data ONTAP 7.1.x, NetApp supports the `dns.update.enable` option for Dynamic DNS.

When using DNS servers not based on Windows 2000, such as Berkeley Internet Name Domain (BIND) servers, verify that the version being used supports SRV records or update it to a version that does.

6.2 DOMAIN CONTROLLERS DISCOVERY

When deployed in a Microsoft Windows Active Directory environment, NetApp storage systems must be able to locate, prioritize, and select a number of services running on Windows servers. Data ONTAP software does this by executing a selection process that establishes connections to domain controllers (DCs), LDAP, KDC, and KPASSWD services. The storage system attempts to search for domain controllers or LDAP servers under the following conditions:

- The storage system has been started or rebooted.
- A CIFS `resetdc` command has been issued.
- Four hours have elapsed since the last search.

For Active Directory environments, site membership is one of the criteria by which the storage system selects domain controllers (when no preferred domain controllers are available). Therefore, it is important to have the sites and services configured properly (with the storage system's subnet information included in the same site as the storage system).

Data ONTAP performs the following discovery process for the domain controllers and LDAP servers. Figure 2 illustrates the domain controller discovery and selection process in a flowchart.

1. Verify the cached server address bias (“last connection” cache).
2. Verify the domain controller priority groups:
   - Preferred: Domain controllers defined in the `cifs prefdc` list
   - Favored: Domain controllers that are members of the same Active Directory site or that share the same subnet as the storage system sorted by either the fastest response time or in random order
   - Other: Domain controllers that are not members of the same Active Directory site sorted by either the fastest response time or in random order
3. Query directory SRV records in DNS.

Note: Site membership is specific to Active Directory domains; therefore, there is no Favored category for Windows NT 4 domains or for mixed-mode domains in which your NetApp system is configured as a Windows NT 4 server. In these environments, all domain controllers found through discovery are assigned to the Other category.

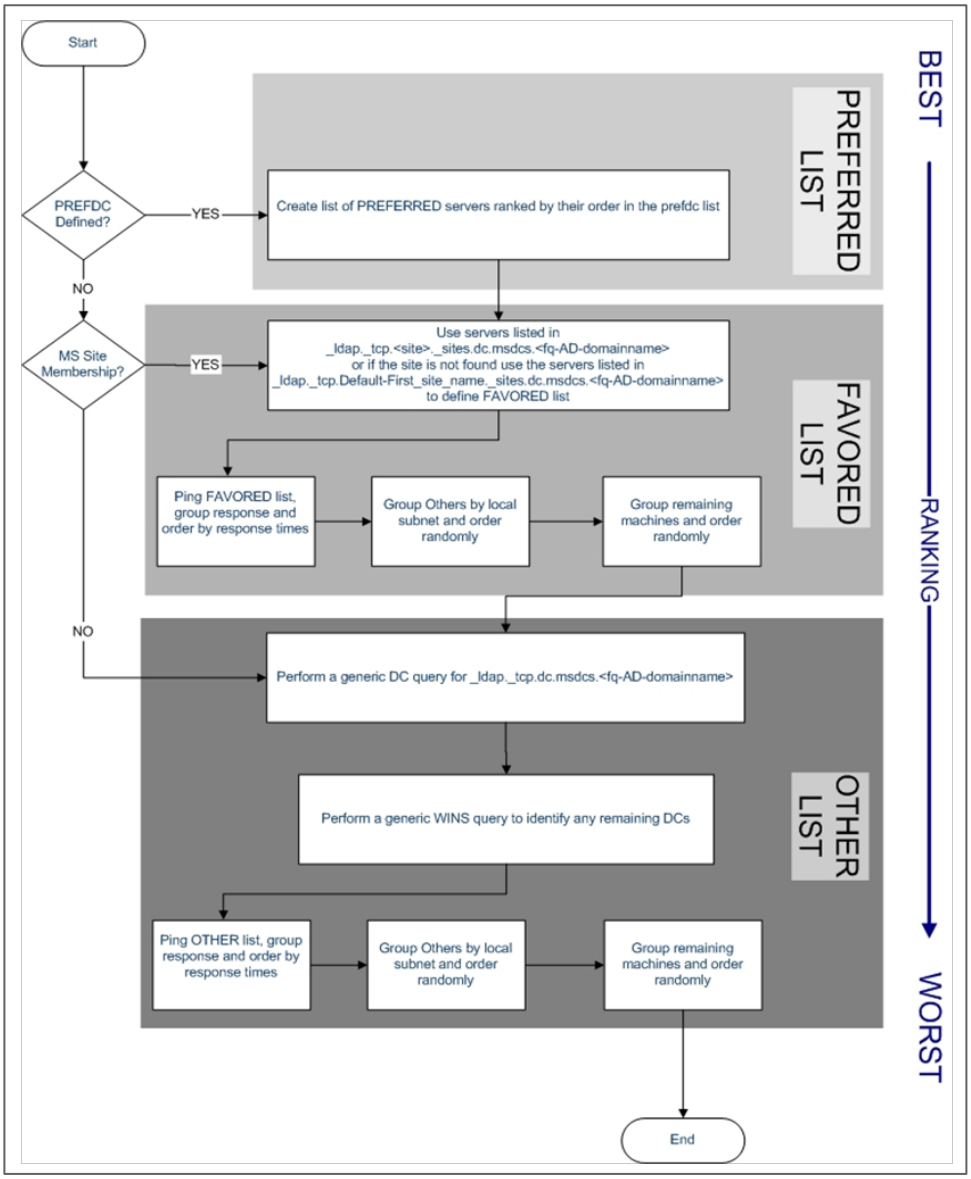
If the NetApp storage system cannot locate an Active Directory domain controller, it switches to Windows NT 4 mode and searches for a Windows NT 4.0 domain controller by using the Windows Internet Naming Service and NetBIOS protocol or by using b-node broadcasts. If the storage system is configured in or switches to Windows NT 4 mode, the following conditions apply:

- Storage systems can register each interface with the Windows Internet Naming Service. (The Windows Internet Naming Service registration can be turned on or off on each interface.)
- Storage systems authenticate incoming sessions against a Windows domain controller by using the Windows NT LAN Manager authentication protocol.

If the NetApp storage system can locate an Active Directory domain controller, the following conditions apply:

- Clients obtain their session credentials by contacting a domain controller/Kerberos key distribution center (DC/KDC).
- CIFS/SMB is supported on TCP port 445.
- Registering with Windows Internet Naming Service servers is optional and can be turned on or off on each network interface.

Figure 2) Domain controller discovery and selection flowchart.



6.3 ACTIVE DIRECTORY SITE AWARENESS

Active Directory sites are used to logically represent an underlying physical network. A site is a collection of networks connected at LAN speed. Slower and less reliable wide area networks (WANs) are used between sites (locations) that are too far apart to be connected by a LAN.

NetApp storage systems are Active Directory site aware. Therefore, they attempt to communicate with a domain controller in the same site instead of selecting a domain controller at a different location. It is important to place the NetApp storage system in the proper Active Directory site to use resources that are physically close to it. To check the site information on a NetApp system, use the `cifs domaininfo` command.

6.4 SMB SIGNING SUPPORT

Data ONTAP supports Server Message Block (SMB) signing when requested by the client. SMB signing helps to make sure that network traffic between the storage system and the client has not been compromised by preventing “man in the middle” attacks.

When SMB signing is enabled on the storage system, it is the equivalent of the Microsoft network server policy “Digitally sign communications (if client agrees).” It is not possible to configure the storage system to require SMB signing communications from clients, which is the equivalent of the Microsoft network server policy “Digitally sign communications (always).” SMB signing is disabled by default on the storage system for performance reasons. To enable this option, turn on `options cifs.signing.enable`.

Most Windows clients negotiate SMB signing by default if it is enabled on the server. When SMB signing is enabled, the performance of all CIFS communications to and from the Windows clients is significantly affected. This in turn affects both the clients and the server (the storage system running Data ONTAP). The performance degradation shows as increased CPU usage on both the client and the server, although the amount of network traffic does not change.

Depending on your network and your storage system implementation, the performance impact of SMB signing can vary widely and can be verified only through testing in your network environment. If you require SMB protection for some of your Windows clients, and if SMB signing is causing performance issues, you can disable SMB signing on any of your Windows clients that do not require protection against replay attacks.

Note: To enable SMB signing for SMB 2.0 protocol, turn on `options cifs.smb2.signing.required`.

6.5 LDAP SIGNING AND SEALING SUPPORT

Signing Lightweight Directory Access Protocol (LDAP) traffic makes sure that the packaged data comes from a known source and that it has not been tampered with. Sealing is the encryption of all the LDAP traffic. Beginning with Data ONTAP 7.0.1, LDAP signing and sealing are supported on NetApp storage systems.

6.6 SPARSE FILE ATTRIBUTE SUPPORT

Sparse files allow programs to create very large files, but to consume disk space only as needed. A sparse file is a file with an attribute that causes the I/O subsystem to allocate the file's meaningful (nonzero) data. All nonzero data is allocated on disk, whereas all nonmeaningful data (large strings of data composed of zeros) is not. When a sparse file is read, allocated data is returned as it was stored, and nonallocated data is returned, by default, as zeros in accordance with the C2 security requirement specification. Beginning with Data ONTAP 7.3, the NTFS Sparse File Attribute is supported on NetApp storage systems.

7 AUTHENTICATION

NetApp storage systems can operate in Windows workgroup mode or Windows domain mode. Workgroup authentication allows local Windows client access and does not rely on a domain controller. In domain authentication, the client negotiates the highest possible security level when a connection to the storage system is established. Two primary levels of security can be chosen:

- **Basic security.** Based on Windows NT LAN Manager (NTLM) or NTLMv2
- **Extended security.** Uses Windows 2000 Kerberos implementation

During the session-setup sequence, Windows computers negotiate which authentication methods are supported. Windows 2000 and Windows 2003 computers that are not part of an Active Directory domain

use only NTLM-based authentication. By default, Windows 2003, Windows XP, and Windows 2000 computers that are part of an Active Directory domain try to use Kerberos authentication first and then NTLM-based authentication. Windows NT 4.0, Windows NT 3.x, and Windows 95/98 clients always authenticate using NTLM-based authentication.

Data ONTAP includes native implementations of the NTLM and Kerberos protocols and thus provides full support for the Active Directory and legacy authentication methods.

7.1 KERBEROS AUTHENTICATION

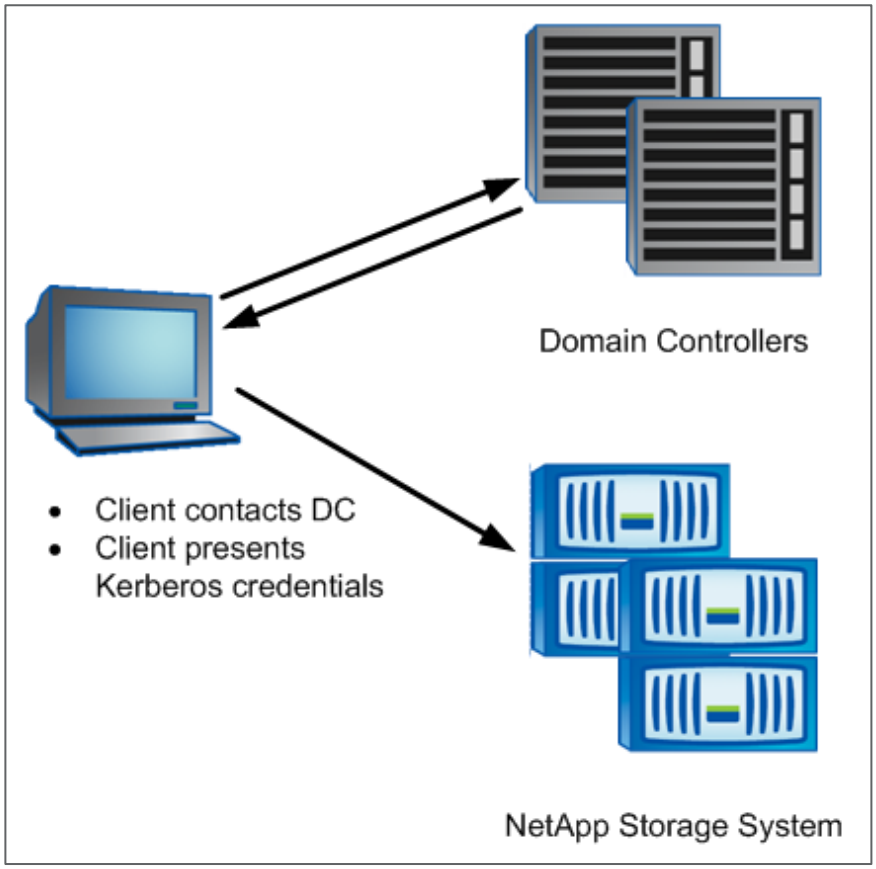
The Kerberos server, or Kerberos Key Distribution Center (KDC) service, stores and retrieves information about security principles in the Active Directory. Unlike the NTLM model, Active Directory clients (users) who want to establish a session with another computer, such as a storage system, contact a KDC directly to obtain their session credentials.

Using Kerberos, clients contact the KDC service that runs on Windows 2000, Windows 2003, Windows 2008, or Windows 2008R2 domain controllers. The client asks for admission to the Ticket Granting Ticket (TGT) for the domain. This is an authentication service exchange between the Kerberos SSP and the KDC on the user's domain (KRB_AS_REQ and KRB_AS_REP). The result is a TGT that the client can use to request session keys to services.

The client uses the TGT to ask for admission to the NetApp storage system's domain. This is a Ticket Granting Service (TGS) exchange between the Kerberos SSP on the computer and the KDC for the computer's account domain (KRB_TGS_REQ and KRB_TGS_REP). The result is a session ticket that the client can present when requesting access to the system services on the computer. Clients then pass the authenticator and encrypted session ticket to the storage system, as shown in Figure 3.

For more information on Kerberos authentication, refer to TR-3457: Unified Windows and UNIX Authentication Using Microsoft Active Directory Kerberos.

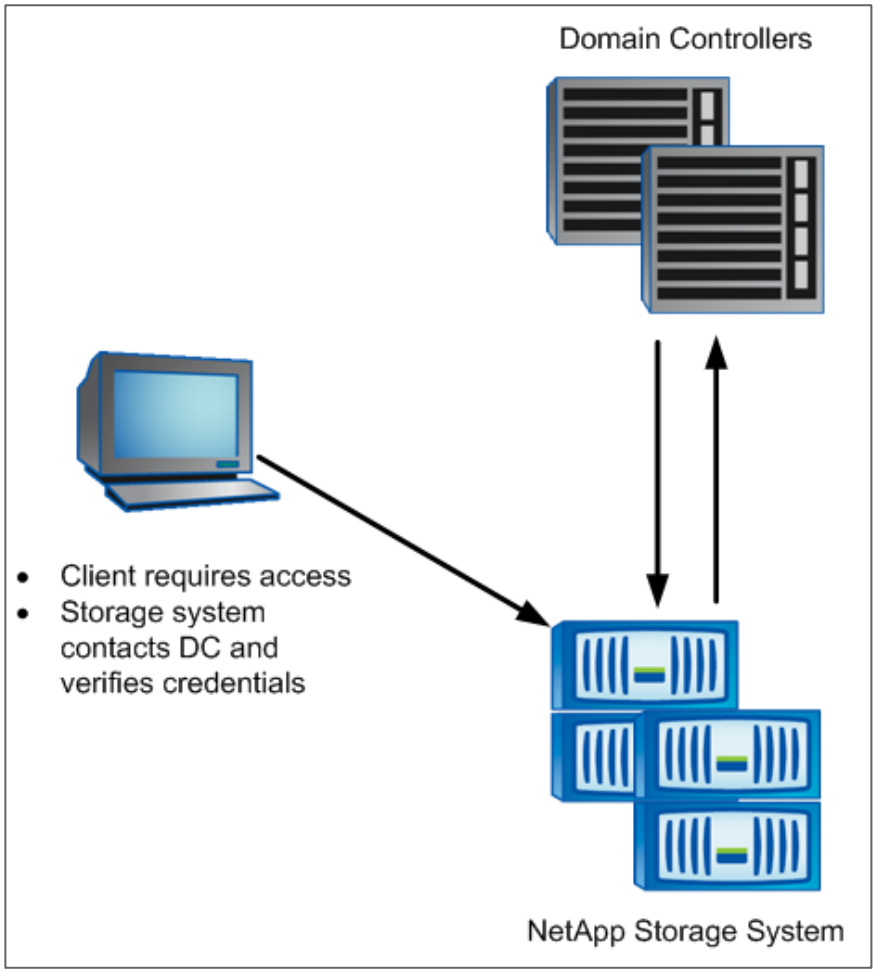
Figure 3) Microsoft Windows 2003 Kerberos authentication.



7.2 MICROSOFT WINDOWS NT LAN MANAGER AUTHENTICATION

By using NTLM, the NetApp storage system contacts the Windows NT 4.0, Windows 2000, Windows 2003, Windows 2008, or Windows 2008R2 domain controller to verify a user's supplied credentials, which consist of a user name, a challenge sent to the client, and a response received from the client. The domain controller retrieves the user's password from the Security Account Manager database and uses it to encrypt the challenge. The domain controller then compares that encrypted challenge with the response computed by the client. If these are identical, the NTLM authentication is successful. Then the domain controller sends the response back to the storage system for successful authentication, and the storage system allows the user to access the file system based on the access permissions, as shown in Figure 4.

Figure 4) NT LAN Manager authentication.



7.3 MINIMUM SESSION SECURITY FOR NTLM AUTHENTICATION

Session security for NTLM authentication determines which challenge/response authentication protocol is used for net logons. There are five levels in which to negotiate the challenge/response through `option cifs.LMCompatibilityLevel <level>`:

- **Level 1.** Accept LM, NTLM, NTLMv2 session security, NTLMv2, Kerberos (default).
- **Level 2.** Accept NTLM, NTLMv2 session security, NTLMv2, Kerberos.
- **Level 3.** Accept NTLMv2 session security, NTLMv2, Kerberos.
- **Level 4.** Accept NTLMv2, Kerberos.
- **Level 5.** Accept Kerberos only.

8 INSTALLING A STORAGE SYSTEM IN AN ACTIVE DIRECTORY ENVIRONMENT

When installing a NetApp storage system in a Microsoft Active Directory environment, the following requirements must be met:

- Verify that the storage system is configured with the IP address of a DNS server that meets the requirements for Microsoft Active Directory. This address is usually the IP address of a DNS server that is authoritative for the Windows domain in which the NetApp system joins.
- Manually create a host (or "A" address) record for the storage system in DNS.
- Match the storage system's time and time zone settings to those on the domain controller. Usually, a best practice is to use one or more NTP servers and configure the timed options on the NetApp system. NetApp also recommends using either the fully qualified hostname or the IP address of the NTP servers.

Caution

If the time settings on the storage system and the domain controller are more than five minutes apart, the installation fails. (The Kerberos protocol requires that the time settings on the storage system and domain controller be nearly the same.)

- Have access to an account in the domain that has rights to add a computer to the domain.
- Select the Active Directory container or organizational unit (OU) in which the storage system's machine account will reside. By default, this is the computer's OU.

9 MANAGING HOME DIRECTORIES

NetApp storage systems are commonly used to store an organization's personal home directories for a variety of compelling reasons. One significant benefit of having the CIFS home directories on a NetApp storage system is that it eases the administration of the storage system by creating only one share that resolves the location of all the users' home directories. Users are offered a dynamic share with their matching directory name. From the CIFS client perspective, the home directory works the same way as any other share to which the user can connect. Each user can see and connect only to his or her home directory, not the home directories for other users.

One disadvantage of having thousands of home shares for individual users is that it can affect the takeover/giveback time on a clustered system. It can take up to five minutes or longer until the CIFS is initialized, depending on the number of shares. Compared to the traditional method, in which administrators have to create one share per user, the NetApp home directories feature uses fewer system resources and therefore improves overall system performance.

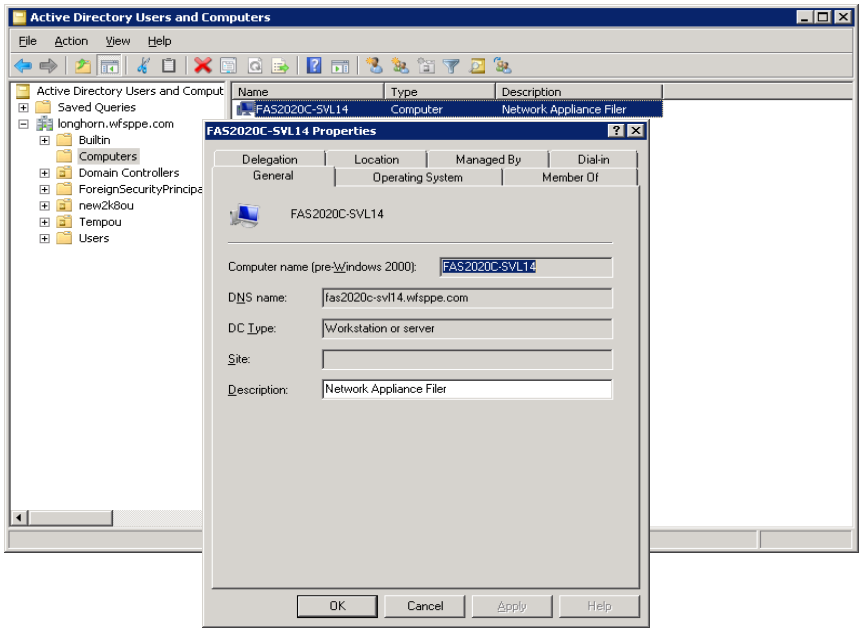
You can also specify multiple home directory paths (up to 1,000) for users in a large enterprise environment. Data ONTAP searches in all of these paths sequentially to match a user's home directory and stops searching when it finds the matching directory.

For more information on configuring and managing home directories on NetApp storage systems, refer to Managing Home Directories on the NetApp Support (NOW) Web site.

10 ADMINISTERING A STORAGE SYSTEM USING A WINDOWS COMPUTER

By default, NetApp storage systems are installed under the Computers organizational unit in Active Directory. Figure 5 shows how to use Active Directory for users and computers to provide a description, manage the security permissions, and look at other computer object properties for a NetApp storage system in the Active Directory Microsoft Management Console (MMC).

Figure 5) Using Active Directory computer management.



10.1 USING THE COMPUTER MANAGEMENT MMC TO ADMINISTER THE STORAGE SYSTEM

Administrators can use the Computer Management MMC from any Windows computer in the domain to perform the following common administration tasks on a NetApp storage system:

- Create a share on the storage system.
- Create a local group on the storage system.
- Add users to or remove them from a local group.
- Manage the CIFS sessions on the storage system.

Figure 6, Figure 7, and Figure 8 illustrate how to create shares, manage local groups, and manage CIFS sessions using the Computer Management MMC.

Figure 6) Creating a CIFS share on a storage system.

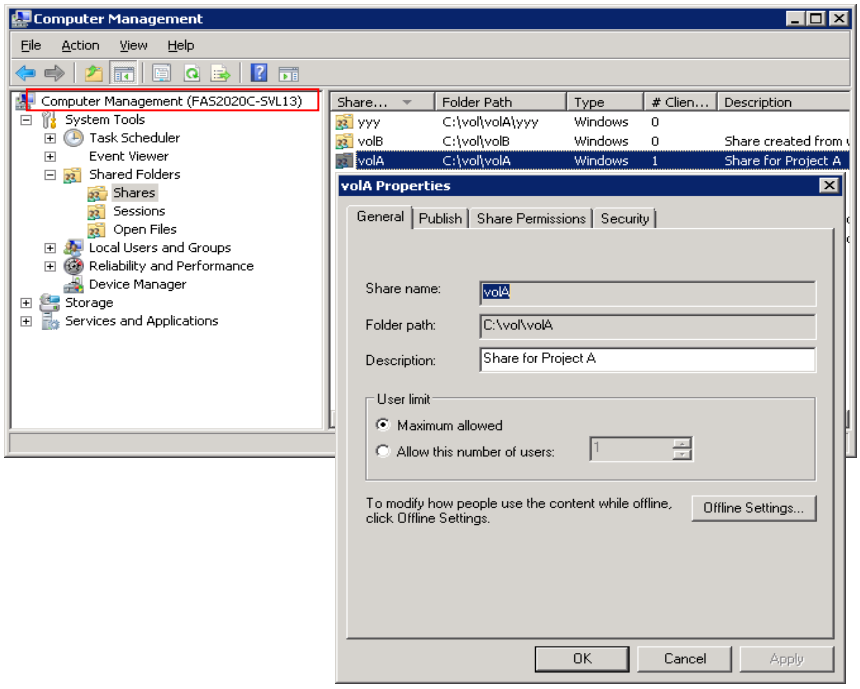


Figure 7) Managing a CIFS session on a storage system.

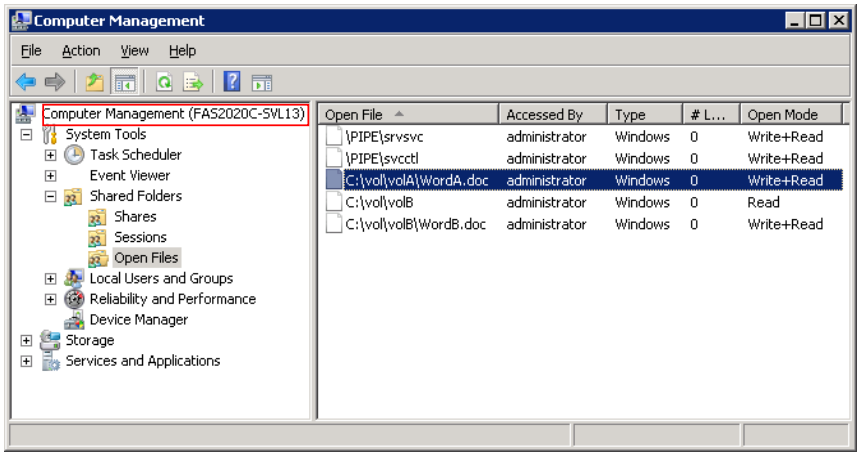
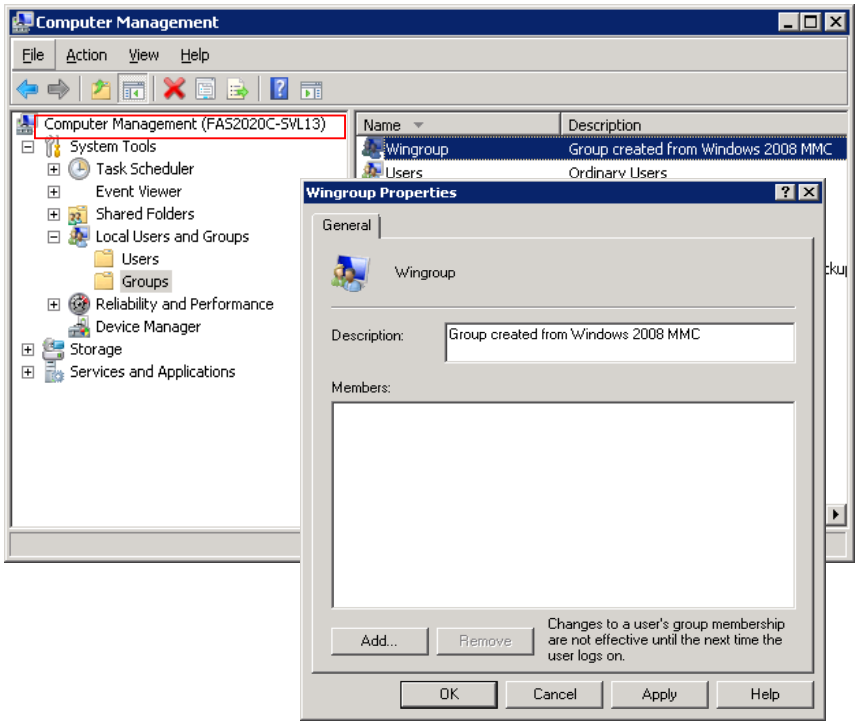


Figure 8) Managing local groups on a storage system.



10.2 USING THE ACTIVE DIRECTORY MMC TO MANAGE USERS

NetApp storage systems fully support the users and group database stored in Active Directory, including the roaming profiles and Windows home directories for users.

ROAMING PROFILES

If a computer is running Windows Server 2008R2, Windows Server 2008, Windows Server 2003 (R2), or Windows Server 2000 on a network, users can store their profiles on the server. These profiles are called roaming user profiles.

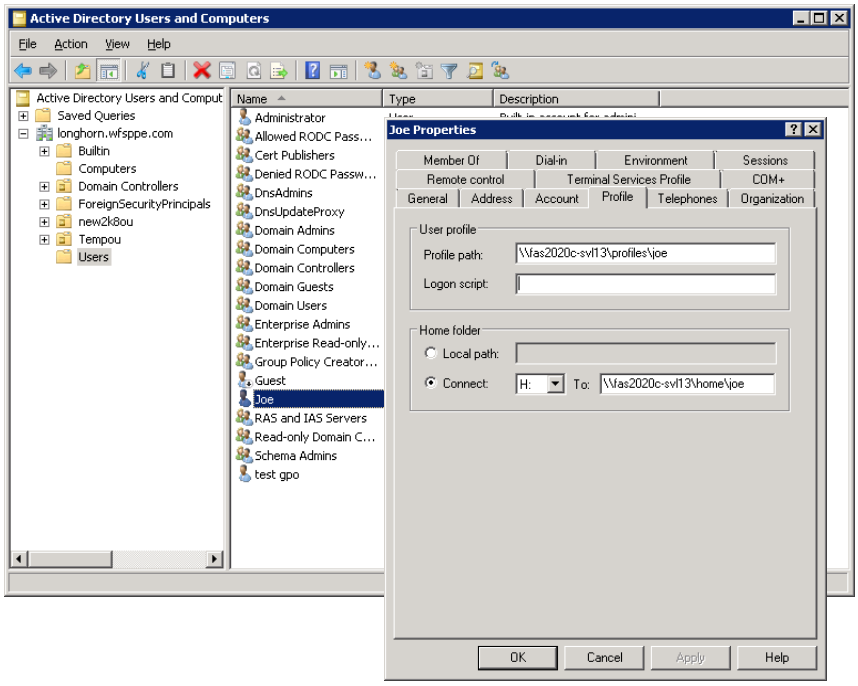
Roaming user profiles have the following advantages:

- **Automatic resource availability.** A user's unique profile is automatically available when that user logs on to any computer on the network that is running Windows 7, Windows Vista, Windows 2000, or Windows XP. Users do not need to create a profile on each computer they use on a network.
- **Simplified computer replacement and backup.** A user's computer can be replaced easily because all of the user's profile information is maintained separately on the network, independent of an individual computer. When the user logs on to the new computer for the first time, the server copy of the user's profile is copied to the new computer.

For more information, refer to Configuring Roaming User Profiles for Windows 2003 and the Managing Roaming User Data Deployment Guide for Windows Vista.

Administrators can use Active Directory to create users and to specify their user profiles and the home directories that reside on storage systems. Figure 9 shows how to create a roaming profile on a storage system for a user using the Active Directory Users and Computers MMC.

Figure 9) Using the Active Directory MMC to manage users.



10.3 APPLYING GROUP POLICY OBJECTS

To enable additional management in Active Directory, Group Policy Objects (GPOs) can be applied to users, computers, and servers in the domain. A GPO is a set of rules that are applicable to users and computers in an Active Directory environment, and these rules are defined centrally for ease of administration and increased security. Settings that you control with GPOs include environmental settings, user rights assignment, account policies, folder redirection, script assignment, security settings, and software distribution.

Beginning with Data ONTAP version 6.4, NetApp storage systems fully support GPOs that apply to users and users' computers. Although few GPOs are applicable to a NetApp storage system, it is able to recognize and process a certain set of GPOs.

The following GPOs are currently supported:

- Start-up and shut-down scripts
- The GPO refresh time interval for computers
- File system security settings
- Restricted group security
- Event log support
- Auditing support
- User rights assignment
- GPO refresh time interval random offset

GPO support can be easily enabled on a NetApp storage system by setting an option in Data ONTAP using the graphical user interface (GUI) for storage system administration. The CLI for enabling this option is:

```
options cifs.gpo.enable on | off
```

Make sure that CIFS is licensed and configured on the storage system and that it is already associated with an Organizational Unit (OU).

MANAGING GPOS

To display GPOs that are currently in effect for the storage system and the results of those GPOs, use the `cifs gpresult [ -r | -v | -d]` command, which simulates the output of the Windows 2000/XP `gpresult.exe /force` command.

Group policy settings on the storage system can be updated in three ways:

- **All GPOs are verified every 90 minutes.** By default, Data ONTAP queries Active Directory for changes to GPOs. If the GPO version numbers recorded in Active Directory are higher than those on the storage system, Data ONTAP retrieves and applies the new GPOs. If the version numbers are the same, GPOs on the storage system are not updated.
- **Security settings GPOs are refreshed every 16 hours.** Data ONTAP retrieves and applies security settings GPOs every 16 hours, whether or not these GPOs have changed.

Note: The 16-hour default value cannot be changed in the current Data ONTAP version. It is a Windows default setting.

- **All GPOs can be updated on demand with a Data ONTAP command.** To update GPOs on the storage system with the most current group policy settings available in an Active Directory domain, use the `cifs gpupdate` command, which simulates the Windows 2000/XP `gpupdate.exe /force` command.

SUPPORTED GPOS

How Start-Up and Shut-Down Scripts Are Applied on a Storage System

After the GPOs have been enabled on a storage system and specified in the Active Directory domain, the start-up and shut-down scripts are applied to the storage system in the following way:

1. When the storage system starts, it retrieves GPOs from the domain controller, including the start-up and shut-down scripts information. The storage system runs the retrieved start-up scripts.
2. The storage system accesses the scripts from the domain controller's `sysvol` directory and saves these files locally in the `/etc/ad` directory.

Periodically, the storage system retrieves updates to the start-up and shut-down scripts.

During a shutdown or a reboot, the storage system executes the last retrieved shut-down script.

GPO File System Security Settings

You can specify GPO file system security settings directly on Data ONTAP file system objects (directories or files). These settings are propagated down the directory hierarchy; that is, when you set a GPO security setting on a directory, that setting is applied to objects within that directory. GPO security settings can be used to propagate the inherited permissions or replace the permissions on the child objects.

Note: These file system security settings can be applied only in mixed or NTFS volumes or qtrees. They cannot be applied to a file or directory in a UNIX® volume or qtree. File system security ACL propagation is limited to about 280 levels of directory hierarchy.

Restricted Group Security

Restricted Group provides an important new security feature that acts as a governor for group membership. Restricted Groups automatically provide security memberships for default Windows 2000 groups that have predefined capabilities, such as Administrators, Power Users, Print Operators, Server Operators, and Domain Admins. You can later add any groups that you consider sensitive or privileged to the Restricted Groups security list.

Configuring Restricted Groups enables group memberships to be set as specified. Groups and users not specified in Restricted Groups are removed from the specific group. In addition, the reverse membership configuration option determines that each restricted group is a member of only those groups specified in the Member of column. For these reasons, Restricted Groups should be used primarily to configure membership of local groups on workstation or member servers.

Event Log and Audit Policy Mapping

Event log and audit policy settings are applied differently to storage systems than to Windows systems because the underlying logging and auditing technologies are different. Event log and audit GPOs are applied to storage systems by mapping and setting corresponding Data ONTAP options. The effect of mapping these options is similar but not identical to event log and audit policy settings. For more information, refer to Event Log and Audit Policy Mapping on the NetApp Support (NOW) Web site.

Group Policy Refresh Interval for Computers and the Random Offset

This policy specifies how often the group policy for computers is updated (in the background) while the computer is in use. This policy specifies a background update rate only for group policies in the Computer Configuration folder.

By default, computer group policy is updated in the background every 90 minutes, with a random offset of 0 to 30 minutes. In addition to the background updates, the group policy for the computer is always updated when the system starts. If you select zero minutes, the computer tries to update the group policy every seven seconds. However, because updates might interfere with users' work and increase network traffic, very short update intervals are not appropriate for most installations.

A random offset has been added to the refresh interval to prevent all clients from requesting group policy at the same time. The range of the random offset is from 0 to 1,440 minutes (24 hours). The random offset prohibits all of the servers from polling the domain controllers at the same time.

User Rights Assignment

This type of group policy is used to define the security settings for a local group policy that relates to the assignment of a particular user privilege. Starting with Data ONTAP 7.2.1, the Take Ownership of Files or Other Objects privilege under User Rights Assignment was added into GPO support; for example, take ownership of files or other objects, access this computer from network, back up files and directories, and more.

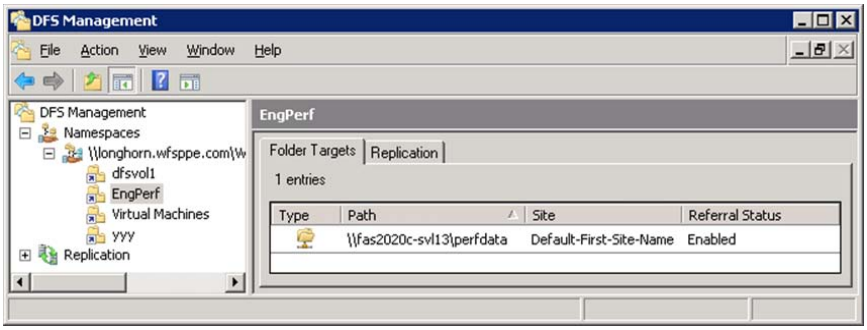
For more information on Group Policy Objects, refer to Applying Group Policy Objects.

10.4 USING WINDOWS DFS MANAGER TO MANAGE LINKS TO SHARES ON STORAGE SYSTEMS

DFS Namespace technology in the Microsoft Distributed File System (DFS) enables you to group shared folders that are located on different servers into one or more logically structured namespaces. Each namespace appears to users as a single shared folder with a series of subfolders. You can use the DFS Management snap-in on a Windows Server to create and manage links to shares on NetApp storage systems, as shown in Figure 10. A NetApp system can participate as a leaf node in both a domain-based and a standalone DFS root. For more information on DFS, refer to Distributed File System on the Microsoft Web site.

Note: VFM® (Virtual File Manager®) is a solution for managing distributed file storage in Windows environments. Built on DFS, VFM enables the integrated management of logical and physical storage elements, making it the most comprehensive Windows storage management solution available. For more information about VFM, refer to the VFM Documentation on the NetApp Support (NOW) site.

Figure 10) Managing links to share on storage systems.



10.5 WIDELINK

Widelink is the NetApp Data ONTAP feature that emulates the Microsoft Distributed File System functionality; it is defined through the `symlink.translations` file.

Widelink is a symbolic link that not only allows the target path to be outside of the share, but also allows path traversal to proceed out of the storage controller. After accessing a widelink object, the storage controller searches the widelink definition in the `symlink.translations` file and returns the DFS referral response to the client. Finally, the DFS-enabled CIFS client is redirected to the target object.

11 MICROSOFT WINDOWS CLIENT FEATURES SUPPORT

Data ONTAP supports many Microsoft Windows client-side features typically used in Microsoft Windows environments. These features are implemented and administered in the same way that customers are familiar with for their existing Microsoft Windows environments.

11.1 ACCESSING AND MANAGING A CIFS SHARE

A Microsoft Windows administrator can create and manage a share on a storage system by using the Microsoft Computer and Users MMC snap-in or by using the following command on the Data ONTAP command line:

```
cifs shares -add shareName path [-comment description]
[-userlimit] [-browse | -nobrowse] [-forcegroup
groupname] [-widelink] [-nosymlink_strict_security] [-
novscan] [-novscanread] [-umask mask] [-no_caching | -
auto_document_caching | -auto_program_caching]
```

For details about all CIFS share options, refer to Sharing Directories.

Figure 6 illustrates how to create and manage a share using the Computer Management MMC.

ACCESS-BASED ENUMERATION

Data ONTAP 7.2 and later releases provide storage system support for access-based enumeration, a shared resource security feature introduced in Microsoft Windows Server 2003 Service Pack 1. This feature allows administrators to control the display of files and folders according to a user's access rights.

Conventional share properties allow you to specify which users (individually or in groups) have permission to view or modify shared resources. However, they do not allow you to control whether shared folders or files are visible to users who do not have permission to access them. This could pose problems if the names of shared folders or files describe sensitive information, such as the names of customers or new products under development.

Access-based enumeration extends share properties to include the enumeration of shared resources. When ABE is enabled on a CIFS share, users who do not have permission to access a shared folder or file underneath it (whether through individual or group permission restrictions) do not see that shared resource displayed in their environment. ABE therefore enables you to filter the display of shared resources based on user access rights.

In addition to protecting sensitive information in your workplace, ABE enables you to simplify the display of large directory structures for the benefit of users who do not need access to your full range of content. ABE can increase worker productivity. End users see only the files and folders that they are responsible for, rather than spending time looking through lists of inaccessible folders and files. Administrators can be more productive because they don't have to help less-skilled users navigate through dense shared folders. With the NetApp implementation of ABE, hardly any performance impact is observed.

ABE for a CIFS share on a NetApp storage system can be managed by the CIFS shares option:

`[-accessbasedenum | -noaccessbasedenum].`

ABE can also be set by the `abecmd.exe` CLI from a Windows system for a CIFS share on a NetApp system:

`abecmd [/enable | /disable] [/server <servername>] {/all | <sharename>}`

Figure 11 and Figure 12 illustrate how ABE affects the Data ONTAP directory listing. In Figure 11, all the folders under the shared customer data folder are visible to the user, even though that user does not have access to some of the folders containing sensitive information. In Figure 12, after enabling access-based enumeration on this share, users can see only the folders to which they have access.

Figure 11) Before enabling the ABE feature on shared customer data.

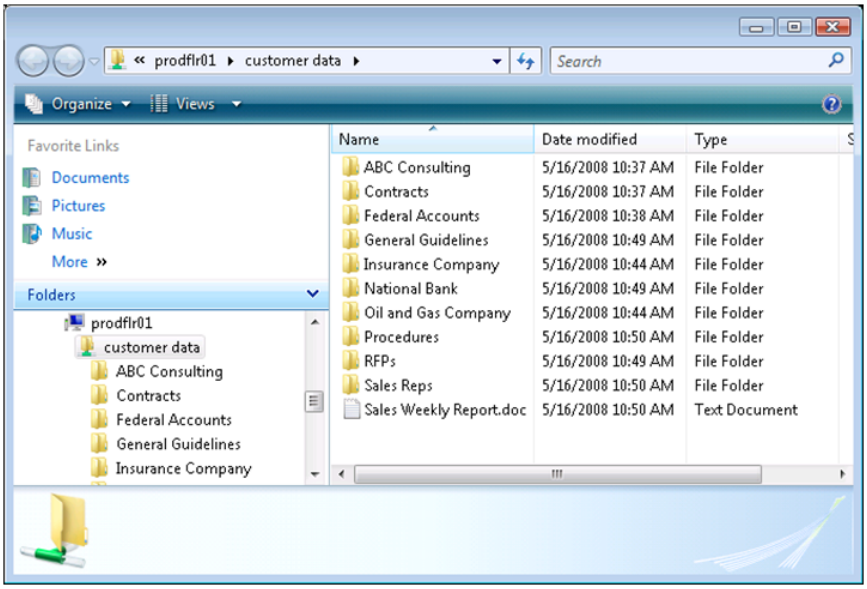
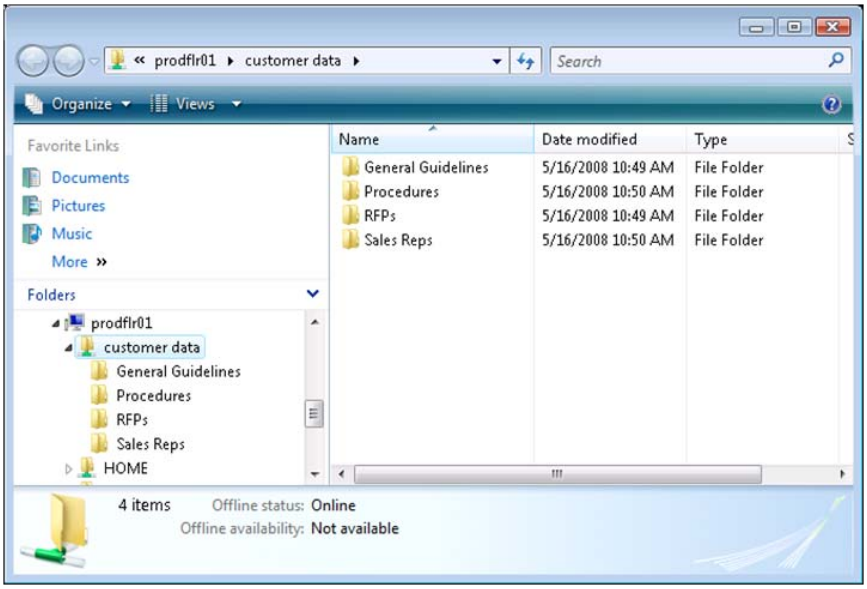


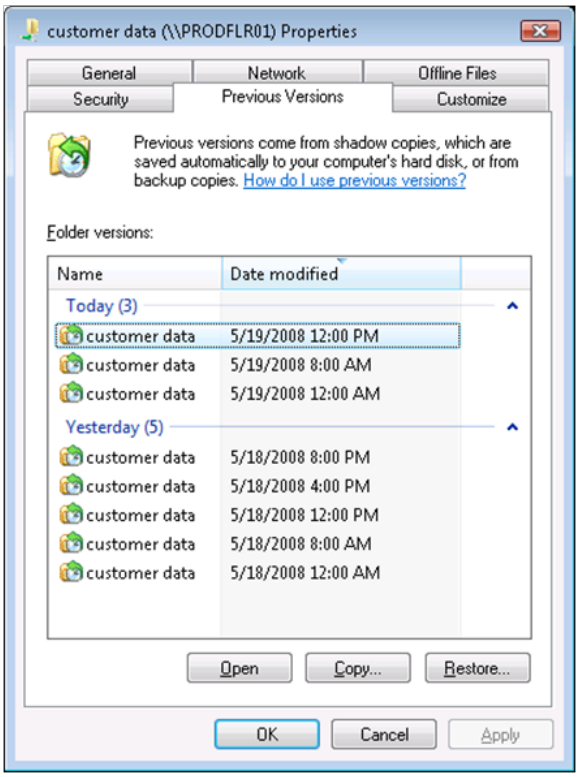
Figure 12) After enabling the ABE feature on shared customer data.



11.2 ACCESSING SHADOW COPIES OF A SHARED FOLDER (VOLUME SHADOW COPY SERVICE CLIENT)

Snapshot technology has been an integral part of the NetApp storage systems solution since 1992. Users can view Snapshot copies created on the storage system by using the Microsoft Volume Shadow Copy Service (VSS) client application. Figure 13 shows how to access shadow copies of a shared folder.

Figure 13) Accessing shadow copies of a shared folder.



11.3 INTELLIMIRROR SUPPORT

OFFLINE FOLDERS (CLIENT-SIDE CACHING)

NetApp storage systems support the Microsoft Offline Folders feature, or client-side caching, which allows files to be cached for offline use on Windows Vista, Windows XP, Windows 2000, and Windows 2003 clients.

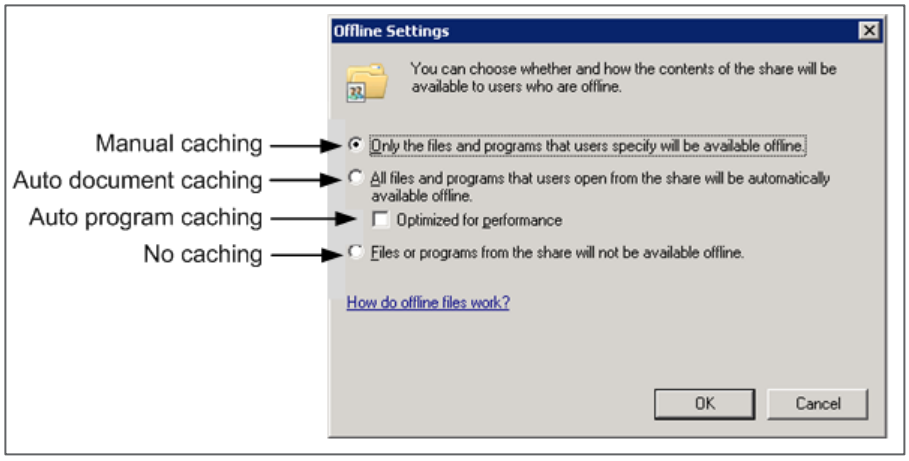
You can also specify whether Windows user documents and programs are automatically cached on a share or whether the files must be manually selected for caching. Manual caching is enabled by default for new shares.

Use the following CIFS shares options to manage client-side caching:

```
[-no_caching | - auto_document_caching | -auto_program_caching]
```

Figure 14 shows the Windows 2008 interpretation of the NetApp storage system caching options.

Figure 14) Microsoft Windows 2008 interpretation of the NetApp storage system caching options.

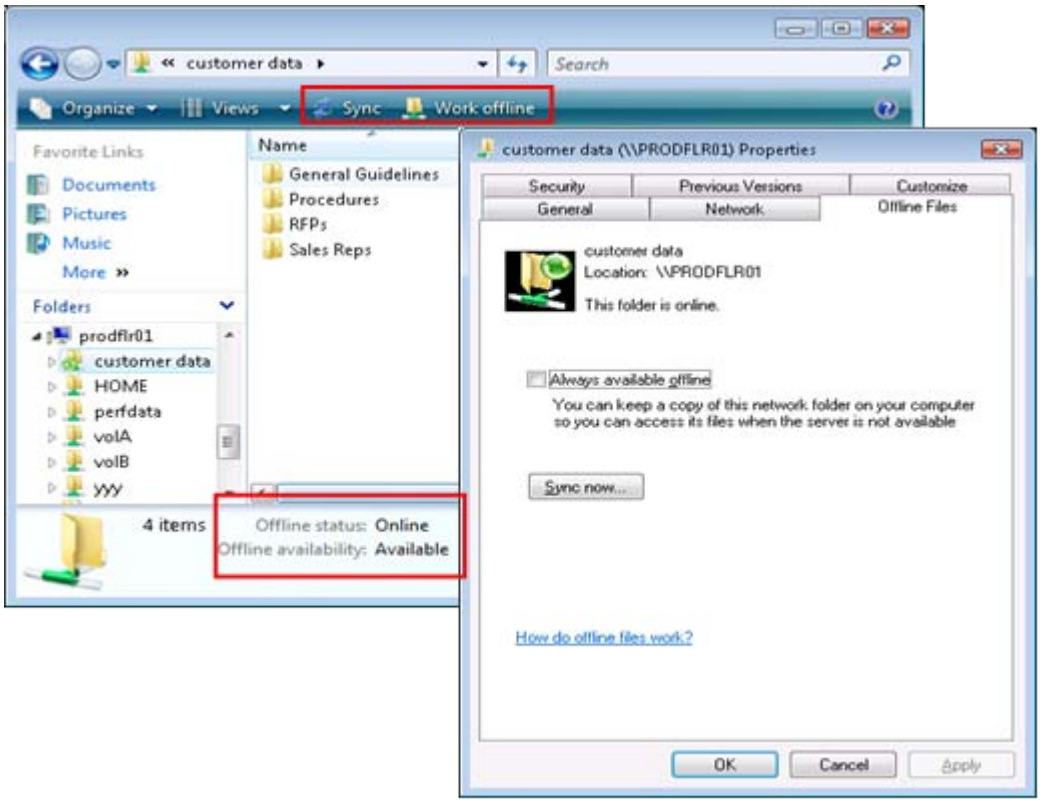


The folders that are made available offline are synchronized to the Windows 2000 local disk. Synchronization occurs when network connectivity to a specific storage system share is restored.

To enable the Offline Folders option on a Windows Vista client in Windows Explorer (as shown in Figure 15):

1. Right-click the folder and select Properties.
2. Click the Offline Files tab.

Figure 15) Enabling offline folders on Windows Vista.



To force this feature on a specific file or folder:

1. Right-click the selected network drive or subfolder.
2. Select Always Available Offline.
3. Refer to Offline Files for Windows Vista for more information.

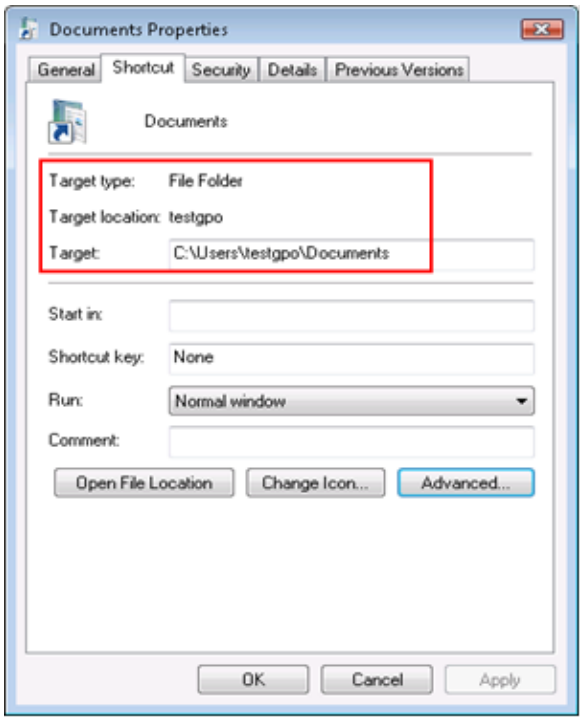
This option is useful for caching large executables on clients (for example, the CATIA V5 CAD application) and to allow mobile users to have access to their data even when they are not connected to the network.

MY DOCUMENTS FOLDER REDIRECTION

NetApp storage systems support Microsoft folder redirection, one of the key components of Microsoft IntelliMirror technology. This option is intended usually for organizations that have already deployed home directories and that want to maintain compatibility with their existing home directory environment. This option can also be used to redirect user-specific profile folders to an alternate location. Documents, Desktop, and Start Menu are examples of folders you can redirect. Folder redirection provides a way for administrators to divide user data from profile data.

Figure 16 shows how to specify a target for folder redirection on Windows Vista to a share on a storage system.

Figure 16) Specifying a target for redirecting My Documents on Windows Vista.

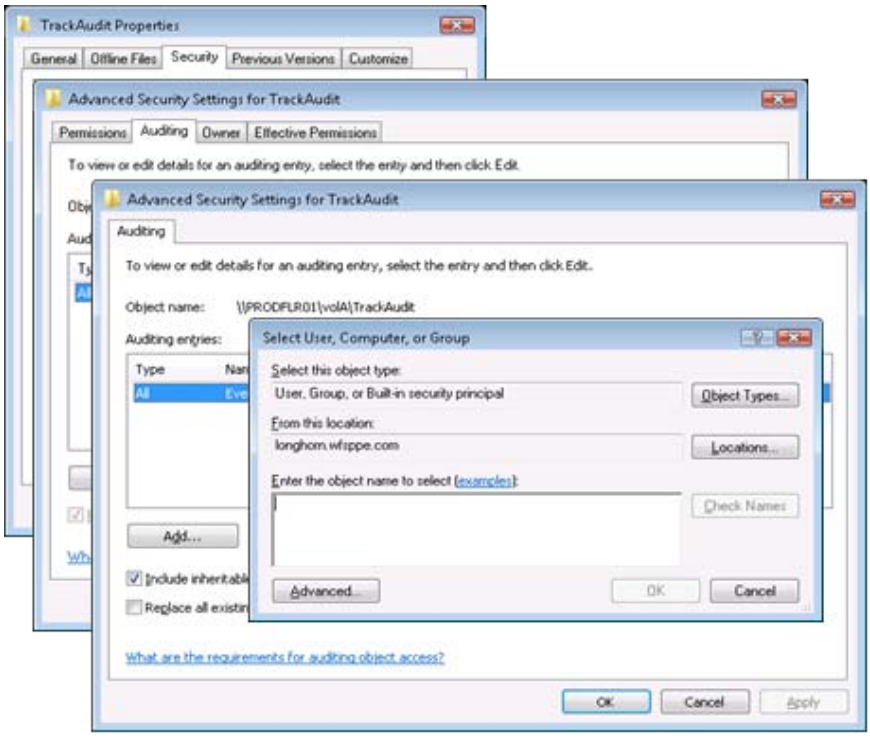


Folder redirection can also be set through a GPO configuration on the Windows Server. For more configuration details, refer to the Managing Roaming User Data Deployment Guide.

11.4 AUDITING EVENT LOG

NetApp storage systems have the ability to audit file and folder access to identify the user who took actions with the various files and directories. The actions are logged in the Microsoft Event View security log format. The mechanism used to provide and manage this feature is the same as that used by Windows file servers. Figure 17 shows how to set an audit on a directory. For more information about configuring CIFS auditing on NetApp storage systems, refer to TR-3595: Auditing Quick Start Guide.

Figure 17) Setting an audit on a directory.



Viewing and Understanding Event Detail Displays

The following types of events are logged and displayed:

- Network logon
- Unsuccessful network logon
- Network logoff
- Windows file access
- UNIX file access
- Unsuccessful file access
- Lost record event
- Clear audit log event

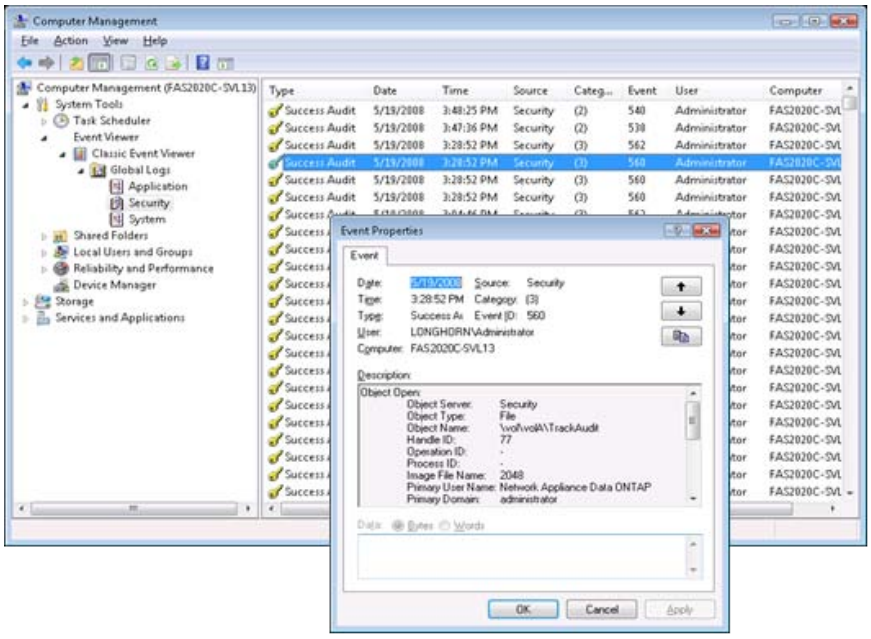
LIVE VIEW: REAL-TIME DISPLAY OF EVENT LOG FILE

Starting with Data ONTAP 7.2, a new feature called Live View was added to CIFS auditing. This feature allows the user to use the Microsoft Event Viewer (an MMC snap-in) and connect to a storage system to retrieve the security audit records in real time. When the Live View feature is enabled, the EVT event log file is automatically saved and refreshed every minute, providing a continuous up-to-date view in Event Viewer of the 5,000 most recent audit events. The Live View feature also manages the log file, providing automatic backup to prevent newer events from overwriting older ones. For more information on configuring Live View, refer to Configuring Live View.

Note: To use the Live View feature, your Windows client must be Windows 2000 or later.

Figure 18 shows the Live View audit log in the Event Viewer by connecting to a storage system. It also shows the display of real-time audit logs.

Figure 18) Real-time display of storage system audit logs through Live View.



STATIC DISPLAY OF THE EVENT LOG FILE

If you do not enable Live View, you must manage the EVT event log by yourself, either manually or by setting up automatic saving options. Therefore, Event Viewer can display only the most recently saved version of the log file contents, depending on how you manage the file.

12 FILE SCREENING

File screening capability allows you to create file screening policies to control the type of data to be stored on the NetApp storage system according to file type. For example, you can restrict certain file types, such as .jpg and .mpg files, from being stored on the storage system. A file policy determines how the storage system handles requests from individual client systems for operations such as open, rename, create, and delete.

There are two ways to enable file screening in Data ONTAP:

- **Using native file blocking.** The file screening software runs natively on the NetApp storage system. Native file blocking provides simple policies for the restricted file types.
- **Using third-party file screening software.** The file screening software runs on a client that functions as a file screening server. The communication between the NetApp storage systems and the file screening server occurs by using the NetApp FPolicy mechanism. The third-party file screening software provides flexible control and filtering of file content. Currently, the supported vendors for file screening servers are Kazeon, NuView, NTP Software, Symantec™ Enterprise Vault™ FSA, and Arkivio. Many uses of FPolicy technology are possible, such as various file-access logging products, quota management, hierarchical storage management, encryption/decryption, compression/decompression, and so on.

Note: For optimal performance, NetApp strongly recommends that the FPolicy server be configured on the same subnet as the storage system.

For more information on the configuration of FPolicy on a storage system, refer to File Screening Using FPolicy.

13 CIFS VIRUS PROTECTION

CIFS virus protection is a Data ONTAP feature that allows a virus-scanning PC client running compliant antivirus applications to provide on-access virus scanning of files on a storage system. On-access virus scanning means that a file is scanned before a CIFS client is allowed to open it.

NetApp has partnered with Symantec, Trend Micro, McAfee, Sophos, and Computer Associates to deliver integrated antivirus solutions.

CIFS virus scanning is carried out on dedicated PC clients running the antivirus application of your choice that is compliant with Data ONTAP. When you enable the virus-scanning process through Data ONTAP on the storage system, the virus-scanning application tells the system to send file-scanning requests.

The virus-scanning application watches for requests from the storage system. Whenever a file of any of the types that you specify is opened or changed on the storage system, Data ONTAP sends the PC client a request to scan the file.

The Data ONTAP virus-scanning process can scan multiple storage systems from a single PC client if your virus-scanning application performs this function. For more information about whether a specific virus-scanning application can accommodate scanning multiple systems, contact the manufacturer of your virus-scanning application.

For more information, refer to TR-3107: Antivirus Scanning Best Practices Guide.

14 CONCLUSION

NetApp storage systems are built on the principles of simplicity, scalability, high data availability, and easy integration with the existing environment. The storage systems support a broad range of Microsoft Windows client types and client features, fully leverage the management and authentication framework provided by Active Directory, and allow administrators to continue to use the native Microsoft administration tools with which they are familiar. As a result, the storage systems better protect information assets, dramatically simplify the file-serving environment, and increase overall corporate productivity.

15 REVISIONS

Date	Name	Description
April 2011	Bingxue Cai	Revised for Data ONTAP 8.0 7-Mode
January 2009	Reena Gupta	Revised for Data ONTAP 7.3.1
May 2008	Reena Gupta	Revised for Data ONTAP 7.3
November 2006	Reena Gupta	Revised
December 2004	Jeff Feierfeil	Creation

16 REFERENCES

16.1 NETAPP REFERENCES

- Applying Group Policy Objects

- The NetApp Support site (formerly NOW)
  http://now.netapp.com
- Configuring Live View
- File Screening Using FPolicy
- Sharing Directories
- TR-3107: Antivirus Scanning Best Practices Guide
- TR-3457: Unified Windows and UNIX Authentication Using Microsoft Active Directory Kerberos
- TR-3740: SMB 2.0–Next-Generation CIFS Protocol in Data ONTAP
- VFM Documentation
- Windows File Service Compatibility Matrix

16.2 MICROSOFT REFERENCES

- Configuring Roaming User Profiles
- Distributed File System
- Offline Files for Windows Vista
- Managing Roaming User Data Deployment Guide
- www.microsoft.com

NetApp provides no representations or warranties regarding the accuracy, reliability, or serviceability of any information or recommendations provided in this publication, or with respect to any results that may be obtained by the use of the information or observance of any recommendations provided herein. The information in this document is distributed AS IS, and the use of this information or the implementation of any recommendations or techniques herein is a customer's responsibility and depends on the customer's ability to evaluate and integrate them into the customer's operational environment. This document and the information contained herein may be used solely in connection with the NetApp products discussed in this document.

www.netapp.com

© 2011 NetApp, Inc. All rights reserved. No portions of this document may be reproduced without prior written consent of NetApp, Inc. Specifications are subject to change without notice. NetApp, the NetApp logo, Go further, faster, Data ONTAP, NOW, SnapRestore, Snapshot, VFM, Virtual File Manager, and WAFL are trademarks or registered trademarks of NetApp, Inc. in the United States and/or other countries. Active Directory, Microsoft, Vista, Windows, and Windows NT are registered trademarks of Microsoft Corporation. UNIX is a registered trademark of The Open Group. Symantec and Enterprise Vault are trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such. TR-3367