Data ONTAP®: Best Practices for Secure Configuration

NetApp Appliance, Inc. | January 2006 | TR-3445

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.

Abstract

This paper provides guidelines on secure configuration of NetApp systems (including storage system and NearStore® systems) running Data ONTAP. It is intended for storage and security administrators who wish to improve the overall security posture of their storage networks. For each configuration area, only the **most secure** settings are provided. Just as with any other information technology, an improvement in the overall level of security may result in a reduction in functionality or usability; put another way, most security problems can be viewed as *excess functionality*, and administrators should be cautious when applying these configurations to avoid interruption of required services.

The second part of this paper provides a high-level discussion of Data ONTAP security concepts within the context of a documentation map that should allow security administrators to develop a good working knowledge of Data ONTAP security, even if they have no prior storage management experience.

Table of Contents

Best Practice Security Configuration 3
Administrative Access 3
NFS Settings 4
CIFS Settings 5
Multiprotocol Settings 6
Network Configuration 7
System Services 8
iSCSI Settings 9
Security Documentation Map 9
Administrator Guidance 10
User Guidance 13

Best Practice Security Configuration

This section provides specific settings and option values that may be used to configure a Filer or NearStore system in the most secure possible fashion. Note that many of the settings described below are already set to the most secure value by default and thus do not require modification on a new system; however, the complete list is provided to assist in auditing systems that have already been deployed.

Administrative Access

Filer Configuration: Administrative Access	
ROOT PASSWORD	
Description	Sets the password for the root account.
Recommended Setting	Use a strong password for the root account.
Procedure	`Filer# passwd root [password]`
TRUSTED HOSTS ACCESS	
Description	Enables/disables the ability for certain hosts to access NetApp storage system without authentication.
Recommended Setting	Disable the trusted host option.
Procedure	`Filer# options trusted.hosts -`
TELNET ACCESS	
Description	Enables/disables telnet access to the filer.
Recommended Setting	Disable telnet access.
Procedure	`Filer# options telnet.enable off`
RSH ACCESS	
Description	Enables/disables RSH access to the filer.
Recommended Setting	Disable RSH access.
Procedure	`Filer# options rsh.enable off`
HTTP ACCESS	
Description	Enables/disables HTTP (Web) access to the filer.
Recommended Setting	Disable HTTP (Web) access.
Procedure	`Filer# options httpd.admin.access host=none`
SECUREADMIN™	
Description	Enables SecureAdmin for SSH and SSL security features.
Recommended Setting	Install SecureAdmin.

Procedure	`filer# secureadmin setup –f ssh`
	`filer# secureadmin enable ssh`
	`filer# secureadmin setup ssl`
	`filer# secureadmin enable ssl`

RESTRICT SSH LOGINS	
Description	Filters' access to SSH to only authorized SSH clients.
Recommended Setting	Limit access to the filer to authorized SSH clients only.

Filer Configuration: Administrative Access	
Procedure	`Filer#` **`options ssh.access host=[ipaddress],[ipaddress],[hostname]`**
NONROOT USERS	
Description	Creates additional accounts on the filer.
Recommended Setting	Create nonroot user accounts for each administrator.
Procedure	`Filer#` **`useradmin useradd [username]`**
AUTOMATIC LOGOUT	
Description	Enables and sets an automatic logout for console and network sessions to the filer.
Recommended Setting	Enable automatic logoff. The specific number of minutes you configure should be based on your local security policy.
Procedure	`filer#` **`options autologout.console.enable on`** `filer#` **`options autologout.telnet.enable on`** `filer#` **`options autologout.console.timeout 30`** `filer#` **`options autologout.telnet.timeout 15`**
LOGGING ADMINISTRATIVE ACCESS	
Description	Enables and configures logging for administrative sessions.
Recommended Setting	Enable logging for administrative sessions. The log file size specified depends on your local security policy, but should be large enough to record several days' worth of administrative usage at a minimum. You may wish to set this to a large value (several megabytes, at least) and then adjust the size once you have an understanding of how quickly it fills up in your environment.
Procedure	`filer#` **`options auditlog.enable on`** `filer#` **`options auditlog.max_file_size [logfilesize]`**
HOSTS.EQUIV ACCESS	
Description	File containing trusted remote hosts for access without authentication.
Recommended Setting	Disable host.equiv access.
Procedure	`filer#` **`options httpd.admin.hostsequiv.enable off`**
PASSWORD CHECKS	
Description	Controls whether a check for minimum length and password composition is performed when new passwords are specified.
Recommended Setting	Enable password checks.
Procedure	`filer#` **`options security.passwd.rules.enable on`**

NFS Settings

Filer Configuration: NFS Settings	
KERBEROS	
Description	Enables Kerberos authentication for NFS. Requires NFS clients to support Kerberos.
Recommended Setting	Enabled NFS authentication with Kerberos.
Procedure	`filer#` **`nfs setup`** `[` **`After performing the nfs setup command, edit /etc/exports on the filer to set "sec=krb5", "sec=krb5i" or "sec=krb5p" in the options field of the exported filesystems.`** `]`
IPSEC	
Description	Enables IPSec between NFS clients and the filer.
Recommended	Enable AH authentication and ESP payload encryption between NetApp storage system and

Filer Configuration: NFS Settings	
Setting	clients.
Procedure	N/A
EXPORTS FILE	
Description	Lists file systems on the filer that are exported.
Recommended Setting	Ensure that only data file systems are exports and not administrative file systems, such as /etc. Additionally, ensure all world-readable exports are read only.
Procedure	Examine the **/etc/exports** file on the filer.
NFS OVER TCP	
Description	Enables NFS sessions using TCP packets instead of UDP.
Recommended Setting	Enable NFS over TCP. TCP is generally more secure than UDP and may facilitate use of NFS across firewall boundaries. However, enabling NFS traffic through a firewall opens up so many ports in both directions that in most cases it is better to deploy the NFS clients and servers within the same security zone, rather than to pass the traffic over a firewall.
Procedure	filer# **options nfs.tcp.enable on** filer# **options nfs.udp.enable off**
NFS MOUNT REQUEST	
Description	Enables/disables NFS mount requests over high-numbered ports.
Recommended Setting	Restrict NFS mounts to low-numbered ports only.
Procedure	filer# **options nfs.mount_rootonly on**

CIFS Settings

Filer Configuration: CIFS Settings	
KERBEROS AUTHENTICATION	
Description	Enables AD authentication, which uses Kerberos by default.
Recommended Setting	Use Active Directory authentication to support Kerberos.
Procedure	Select a Microsoft® Active Directory domain during CIFS setup.
SHARE LEVEL PERMISSIONS	
Description	Sets the share level permission on the storage system's CIFS shares.
Recommended Setting	Change the share level ACL to authorized users only and remove "Everyone/Full Control."
Procedure	filer# **cifs access <sharename> [-g] <user|group> <rights>**
AUDIT CIFS ACCESS	
Description	Audits CIFS access.
Recommended Setting	Enable the auditing on CIFS access to the filer.
Procedure	filer# **options cifs.audit.enable on**
ANONYMOUS CONNECTIONS (RESRICT ANONYMOUS)	
Description	Enables/disables anonymous users from listing CIFS shares on the filer.
Recommended Setting	Disable access to CIFS shares and sharenames from unauthenticated users.
Procedure	filer# **options cifs.restrict_anonymous.enable on**
GUEST ACCESS	
Description	Enables/disables CIFS guest access.

Filer Configuration: CIFS Settings	
Recommended Setting	Disable CIFS guest access.
Procedure	`filer# options cifs.guest_account “”`

Multiprotocol Settings

Filer Configuration: Multiprotocol Settings	
IGNORE ACLS	
Description	When on, ACLs will not affect root access from NFS. The option defaults to "off.”
Recommended Setting	Disable the ignoring of any ACLs.
Procedure	`Filer# options cifs.nfs_root_ignore_acl off`
CIFS BYPASS TRAVERSE CHECKING	
Description	When on (the default), directories in the path to a file are not required to have the 'X' (traverse) permission. This option does not apply in UNIX® qtrees.
Recommended Setting	Enable traverse checking by turning this option off.
Procedure	`Filer# options cifs.bypass_traverse_checking off`
CIFS GID CHECKS	
Description	This option affects security checking for Windows® clients of files with UNIX security, where the requestor is not the file owner. In all cases, Windows client requests are checked against the share-level ACL, and then if the requestor is owner, the "user" perms are used to determine the access permissions. If the requester is not the owner and if **cifs.perm_check_use_gid** is **on** it means files with UNIX security are checked using normal UNIX rules, i.e. if the requester is a member of the file's owning group, the "group" perms are used; otherwise, the "other" perms are used. If the requester is not the owner and if **cifs.perm_check_use_gid** is **off**, files with UNIX security style are checked in a way that works better when controlling access via share-level ACLs. In that case, the requester's desired access is checked against the file's "group" permissions, and the "other" permissions are ignored. In effect, the "group" perms are used as if the Windows client was always a member of the file's owning group, and the "other" perms are never used.
Recommended Setting	Enable CIFS GID checks to require UNIX style security.
Procedure	`filer# options cifs.perm_check_use_gid on`
DEFAULT NT USER	
Description	Specifies the Windows NT® user account to use when a UNIX user accesses a file with Windows NT security (has an ACL), and that UNIX user would not otherwise be mapped.
Recommended Setting	Set the option to a null string, denying access. **NOTE:** Perform this step **ONLY** on multiprotocol systems that have NFS/CIFS usermapping configured correctly; disabling this access on an NFS-only filer will result in access problems for legitimate users.
Procedure	`filer# options wafl.default_nt_user “”`
DEFAULT UNIX USER	
Description	Specifies the UNIX user account to use when a Windows NT user attempts to log in and that Windows NT user would not otherwise be mapped.
Recommended Setting	Set the option to a null string, denying access. **NOTE:** Perform this step **ONLY** on multiprotocol systems that have NFS/CIFS usermapping configured correctly; disabling this access on a CIFS-only filer will result in access problems for legitimate users.
Procedure	`filer# options walf.default_unix_user “”`
ROOT TO ADMIN MAPPINGS	

Filer Configuration: Multiprotocol Settings	
Description	When on (the default), a Windows NT administrator is mapped to UNIX root.
Recommended Setting	Disable root to admin mappings by default.
Procedure	`filer# options walf.nt_admin_priv_map_to_root off`
CHANGE PERMISSIONS	
Description	When enabled, only the root user can change the owner of a file.
Recommended Setting	Allow only root access to change permissions to files.
Procedure	`filer# options walf.root_only_chown on`
CACHE CREDENTIALS	
Description	Specifies the number of minutes a WAFL® credential cache entry is valid. The value can range from 1 through 20,160.
Recommended Setting	Set the minutes to 10 for cache credentials.
Procedure	`filer# options walf.wcc_minutes_valid 10`

Network Configuration

Filer Configuration: Network Settings	
INCOMING PACKETS	
Description	Checks incoming packets for correct addressing.
Recommended Setting	Enable packet checking for correct addressing.
Procedure	`filer# options ip.match_any_ifaddr off`
MAC FASTPATH	
Description	Filer will attempt to use MAC address and interface caching ("fast path") so as to try to send back responses to incoming network traffic using the same interface as the incoming traffic and (in some cases) the destination MAC address equal to the source MAC address of the incoming data.
Recommended Setting	Disable this option. If enabled, this increases the ability for ARP spoofing and session hijacking attacks.
Procedure	`filer# options ip.fastpath.enable off`
LOGGING PING FLOOD	
Description	Enables/disables logging of ping flood attacks.
Recommended Setting	Enable logging of ping attacks.
Procedure	`filer# options ip.ping_throttle.alarm_interval 5`
SNAPMIRROR® ACCESS	
Description	Sets the IP address and hostname for nodes that can received SnapMirror or SnapVault® backups.
Recommended Setting	Set IP address/hostnames to authorized users for backup.
Procedure	`filer# options snapmirror.access host=[ipaddress],[hostname]`
SNAPMIRROR SOURCE ACCESS	
Description	Enables IP address based verification of SnapMirror destination storage system by source storage system.
Recommended Setting	Enable source address verification.

Filer Configuration: Network Settings	
Procedure	`filer#` **`options snapmirror.checkip.enable on`**
NDMP	
Description	Restricts control and data connections to authorized hosts.
Recommended Setting	Limited backup using NDMP to authorized hosts only.
Procedure	`filer#` **`options ndmpd.access host=[ipaddress],[hostname]`**
NDMP AUTHENTICATION	
Description	Sets the NDMP authentication type.
Recommended Setting	Enabled MD5 authentication for NDMP.
Procedure	`filer#` **`options ndmpd.authtype md5`**
DATAFABRIC® MANAGER	
Description	Version of DataFabric Manager (DFM).
Recommended Setting	Ensure DFM version 3.0 or higher is used,
Procedure	`N/A`

System Services

Filer Configuration: System Services	
FTP	
Description	Enables/disables FTP.
Recommended Setting	Disable FTP.
Procedure	`filer#` **`options ftpd.enable off`**
PCNFS	
Description	Enables/disables PCNFS.
Recommended Setting	Disable PCNFS.
Procedure	`filer#` **`options pcnfs.enable off`**
SNMP	
Description	Enables/disables SNMP.
Recommended Setting	Disable SNMP.
Procedure	`filer#` **`options snmp.enable off`**
RSH	
Description	Enables/disables RSH.
Recommended Setting	Disable RSH.
Procedure	`filer#` **`options rsh.enable off`**
TELNET	
Description	Enables/disables Telnet.
Recommended Setting	Disable Telnet.
Procedure	`filer#` **`options telnet.enable off`**
TFTP	

Filer Configuration: System Services	
Description	Enables/disables TFTP.
Recommended Setting	Disable TFTP.
Procedure	`filer#` **`options tftpd.enable off`**

iSCSI Settings

Filer Configuration: iSCSI Settings	
PER-INTERFACE CONFIGURATION	
Description	Enables/disables iSCSI driver on each network interface.
Recommended Setting	Enable iSCSI only on adapters where you intend to use it.
Procedure	`filer#` **iscsi interface disable [-f] {-a | <interface>…}**
DEFAULT SECURITY METHOD	
Description	Selects the security method to use for initiators that do not have a security method specified.
Recommended Setting	Set the default iSCSI security method to “deny,” disabling access by initiators with no security method defined.
Procedure	`filer#` **iscsi default –s deny**
INITIATOR SECURITY METHOD	
Description	Specifies the security method to be used for each specific iSCSI initiator.
Recommended Setting	Use CHAP authentication for all iSCSI initiators. See the next entry for how to generate a random 128-bit password.
Procedure	`filer#` **iscsi security add –i *initiator* –s CHAP –p *password* –n *name***
RANDOM CHAP PASSWORDS	
Description	Generates a 128-bit random password for use with iSCSI CHAP authentication.
Recommended Setting	Using this or another method of your choice, generate completely random passwords for use with iSCSI CHAP authentication.
Procedure	`filer#` **iscsi security generate**

Security Documentation Map

This section provides an overview of the security-relevant documentation available for Data ONTAP. It is intended to assist security administrators who are not storage experts in quickly learning enough about Data ONTAP security to make good deployment and configuration decisions. This is not an exhaustive list of all possible security resources, but should serve well as a starting point. This documentation map refers to the Data ONTAP 7.0 documentation; however, documentation for other versions of Data ONTAP is organized in a similar manner. Always refer to the documentation for the version of Data ONTAP that you are actually using.

The first section describes the administrative functions and interfaces available to the administrator and how to administer Data ONTAP in a secure manner. The second section describes the limited set of security interfaces and functions available to the users, describes the use of the user-accessible security functions, and includes warnings about user-accessible functions and privileges that should be controlled.

Throughout both sections, frequent references are made to the Data ONTAP 7.0 documentation. This documentation is available on the Network Appliance Web site at http://now.netapp.com/NOW/knowledge/docs/ontap/rel70.

Administrator Guidance

The first step to understanding the security-relevant administrative functions and interfaces of Data ONTAP is to understand the basic steps required to access and manage the Filer or NearStore system. The most important documentation on this subject is chapters 2, 3, 6, and 7 of the System Administration Guide. In particular, pay close attention to the following sections:

Chapter 2: Interfacing with Data ONTAP
- How You Administer a NetApp System

Chapter 3: Accessing the NetApp System
- Managing Access from Administration Hosts
- Controlling System Access

Chapter 6: Managing Administrator Access
- Managing Users
- Managing Roles

Chapter 7: Performing General System Maintenance
- Synchronizing Filer System Time
- Configuring Message Logging
- Configuring Audit Logging
- Maintaining Filer Security through Options

It is important to note that the "users" described in chapter 6 are local and should be created and used only for SYSTEM ADMINISTRATORS, and NOT for normal end users. In other words, when the Data ONTAP documentation refers to “users” or "local users” or “local user accounts,” it should be interpreted as "local ADMINISTRATOR user accounts.” It is possible, in some small workgroup environments, to use these local accounts for normal user access to files; however, there are many security problems with this approach, and customers who wish to use Data ONTAP in a secure manner should not consider it.

Since the security of the administrative interfaces of the filer depends on limiting access to authorized administrators, it is EXTREMELY IMPORTANT that administrator passwords be selected and managed very carefully. Great caution should be exercised to ensure that administrator passwords are difficult to guess; words found in any dictionary or wordlist (including names, dates, place-names, social security or other identifying numbers, etc.) should be avoided. Passwords should contain a mix of uppercase and lowercase letters, punctuation marks, symbols, and numbers. Data ONTAP 7.0 provides an option to check for a minimum length and password composition when a new password is chosen; this option (security.passwd.rules.enable) is enabled by default but is not a substitute for a clear password selection policy and administrator training on correct password selection.

In addition to the administration access methods listed in Chapter 3 ("Accessing the NetApp System") of the System Administration Guide, the Filer may also be managed using the SSH remote login protocol or via an SSL-protected version of FilerView® called Secure FilerView. These two methods are only available if the SecureAdmin product is installed and configured on the Filer. SecureAdmin provides many security advantages over administrative access via telnet, RSH, and HTTP and should be strongly considered by any customer who wants to maximize security. More information on SecureAdmin can be found in Chapter 9 (“Using SecureAdmin”) of the System Administration Guide. Additional documentation for the SecureAdmin 3.0 product is available at http://now.netapp.com/NOW/knowledge/docs/saon/rel30/pdf/secadmin.pdf.

Once administrative access has been configured, the next step for managing a secure Filer is to organize your data. The most important documentation for this process is in Chapter 6 (“Volume Management”) and Chapter 7 ("Qtree Management") of the Storage Management Guide. In particular, pay attention to the following sections:

Chapter 7: Qtree Management
- Understanding Qtrees
- Creating Qtrees
- Understanding Security Styles

- Changing Security Styles

Although the choices for Volume and Qtree security styles may seem confusing at first, the selection process is actually very simple for most customers.

If a volume or qtree is to be accessed predominantly or exclusively by NFS clients, select the "unix" style.
If a volume or qtree is to be accessed predominantly or exclusively by CIFS clients, select the "ntfs" style.
If a volume or qtree is to be accessed equally by both NFS and CIFS clients and both types of clients need full control over file access security, select the "mixed" style.
If a volume or qtree is to be used exclusively as a storage location for FCP or iSCSI LUNs, the security style has no effect.

When creating volumes and qtrees for data management, it is strongly recommended that data be organized by security requirements. For example, if the filer will store data for two groups (maybe the Finance and Engineering departments within a company) with different access controls, placing each data set in a separate qtree or on separate volumes will make security configuration simpler.

After creating and configuring volumes and qtrees to store user data, Data ONTAP must be configured to identify users so that it can control access to data. Documentation about this subject is available in the File Access Management Guide. Note that the users discussed in this chapter are NOT the local administrative users discussed above. Instead, these are the non-administrator users who access data stored by the system using NFS or CIFS.

For security information, the most important sections of this document are:

Chapter 2: File Access Using NFS
- Read the entire chapter, especially the section on providing secure NFS access.

Chapter 3: File Access Using CIFS
- How CIFS Users Obtain UNIX Credentials
- Sharing Directories
- Displaying and Changing Share Properties
- Understanding Authentication Issues
- Understanding Local User Accounts
- How Share-Level Access Control Lists Work
- Specifying How Group IDs Work with Share-Level ACLs
- Changing and Displaying a Share-Level ACL
- Changing and Displaying File-Level ACLs

Chapter 7: File Sharing between NFS and CIFS
- Using LDAP Services
- Installing SecureShare® Access
- Changing UNIX Permissions and DOS Attributes from Windows

An important concept to remember is that there are really two different realms of security to manage when using Data ONTAP for file access; one realm is the security of the Filer or NearStore system running Data ONTAP, including security controls on exported filesystems (for NFS) and shared directories (for CIFS). The other is security of individual files and directories, which is controlled by the individual users who own each file or directory. This control is exercised from NFS clients using the chown and chmod UNIX commands, or from CIFS clients using the procedures in the "Changing and Displaying File-Level ACLs" and "Changing UNIX Permissions and DOS Attributes from Windows" sections. While the first kind of security is entirely controlled by authorized system administrators, the second kind is under the control of each individual nonadministrative user. Thus it is VERY IMPORTANT that users receive training and guidance on what policies and procedures should be followed for setting access controls and permissions on files and directories. Even if the Filer or NearStore system and the Data ONTAP operating system are managed in an entirely secure fashion, a user who sets incorrect ACLs or permissions on a sensitive file may inadvertently compromise the security of the data within that file. Programs must be implemented to ensure constant awareness and education of individual, nonadministrative users on local security policy.

Although Data ONTAP 7.0 provides support for the pc-nfs protocol, it is an inherently insecure protocol and should be avoided.

Since NFS, CIFS, iSCSI, and administrative clients access Data ONTAP over TCP/IP networking, it is important to configure the networking on the Filer or NearStore system in a secure fashion. The most important documentation for this purpose is the Network Management Guide, and in particular the following sections:

- Chapter 3: Network Routing Configuration
  - About Routing in Data ONTAP
    - About Fast Path
- Chapter 4: Host Name Resolution
- Chapter 8: Internet Protocol Security Configuration

In addition to the information supplied in chapter 3, one important configuration for secure deployments of NetApp storage system with multiple network interfaces is the ip.match_any_ifaddr option. By default this option is turned on, which increases performance of the system but also increases exposure to certain types of IP forgery attacks. Turn this option off using the command "options ip.match_any_ifaddr off" on the command line interface.

Whenever possible, Network Appliance Inc. strongly recommends configuring and enabling IPSec as discussed in chapter 8.

For systems configured to provide LUN access via iSCSI, read the Block Access Management Guide for iSCSI. In particular, pay attention to the following security-relevant sections:

- Chapter 4: Managing Igroups
- Chapter 6: Managing the iSCSI Network
  - Managing Security for iSCSI Initiators
  - Managing the iSCSI Service on Filer Interfaces

It is VERY IMPORTANT to enable CHAP authentication for all iSCSI LUNs, and to select strong CHAP passwords.

For systems configured to provide LUN access via FCP, read the Block Access Management Guide for FCP, and in particular Chapter 4 ("Managing Initiator Groups") within that guide.

FCP security may also be enhanced by implementing zoning restrictions on the Fibre Channel switch that may be deployed as part of the configuration; check the documentation for your switch for details. Many switch vendors provide two forms of zoning, known as "hard" and "soft" zoning. Hard zoning is based on the physical port to which a cable is connected and thus provides a better level of security than soft zoning in environments where the switch is in a physically secure location.

Regardless of the types of data stored on the system or which methods are used to access that data, backups must be performed to protect the data in the event of a system failure or other disaster. Data ONTAP provides the capability of backing up data to local tape devices, in which case there are no security considerations, aside from ensuring only authorized administrators gain possession of the backup tapes.

Data ONTAP also provides several methods (SnapMirror, SnapVault, and NDMP) that may be used to perform backups over a TCP/IP network. This kind of network backup has security considerations that must be addressed. The Data Protection Online Backup and Recovery Guide provides information about how to configure security for these kinds of backups, including:

- Chapter 4: Data Protection Using SnapMirror
  - Specifying Destination Filer on the Source Filer
- Chapter 5: Data Protection Using SnapVault
  - Setting Up SnapVault Backup on Open Systems Platforms

- Managing SnapVault Backup of Open Systems Platforms
- Enabling SnapVault

Note that Open Systems SnapVault is a software product that allows data from a Windows, UNIX, or Linux® system to be protected by backing it up to a Filer or NearStore system running Data ONTAP. Security procedures on the Windows, UNIX, or Linux backup client systems (other than SnapVault settings and NDMP) are outside the scope of this document.

The Data Protection Online Backup and Recovery Guide also contains information in Chapter 9 ("Virus Protection for CIFS") on how to provide virus scanning services for files accessed via CIFS. This functionality requires a third party AntiVirus Scanner system from McAfee, Computer Associates, Symantec, , TrendMicro or Sophos. Network Appliance STRONGLY recommends that all customers who use CIFS deploy an antivirus server. An AntiVirus best practice guide – TR3107 can also be found at the following link - http://www.netapp.com/library/tr/3107.pdf.

Information on network-based NDMP tape backups is found in the Data Protection Tape Backup and Recovery Guide. In particular the following sections focus on security relevant features:

Chapter 5: Using NDMP Services
- Managing NDMP Security Features
- Specifying the NDMP Version

User Guidance

For individual end users accessing data stored on a Filer or NearStore system running Data ONTAP, the security configuration options are quite limited because most of the security features and options are controlled by system administrators. In fact, a user accessing data within an iSCSI or FCP LUN has no ability to modify or configure ANY security controls on the Filer or NearStore system.

When accessing files via NFS, most users will be the owner of one or more files or directories. Users may only manage security on files or directories that they own, and only if the NFS filesystem they are accessing is located in a volume or qtree with the "unix" or "mixed" security style. Managing security on a file or directory is performed using the UNIX "chmod" and "chown" commands. Users and administrators should consult the documentation for their UNIX operating system for details on how to use these commands or their equivalents, as the specific syntax and operation can vary between platforms. Users may find that the "chown" command does not function (unless they are logged in as the "root" user) if the Data ONTAP administrator has set the "wafl.root_only_chown" option; this is strongly recommended.

When accessing files via CIFS, most users will be the owner of one or more files or directories. Users may only manage security on files or directories that they own, and only if the CIFS filesystem they are accessing is located in a volume or qtree with the "ntfs" or "mixed" security style. Managing security on a file or directory is performed using the procedures in the "Changing and Displaying a File-Level ACL" section of chapter 3 and "Changing UNIX Permissions and DOS Attributes from Windows" section of chapter 7 in the File Access Management Guide.

Regardless of the methods individual users use to access and manage files stored on the Filer or NearStore system, one must remember an external server in the environment, such as a Kerberos, LDAP, or Microsoft Active Directory server, often performs that user authentication. While it is up to the administrators to keep these servers secure, users must manage their passwords in accordance with local password policies to prevent security incidents.