NETAPP TECHNICAL REPORT

Best Practices for Secure Configuration of Data ONTAP 7G

Roger Weeks, NetApp, Inc.

May 2008 | TR-3649

ABSTRACT

This paper provides guidelines for secure configuration of NetApp® storage systems running Data ONTAP®. It is intended for storage and security administrators who want to improve the overall security of their storage networks. NetApp strongly encourages secure storage design, and this paper provides a framework for such a design. It also describes configuration best practices. Just as with any other information technology, an improvement in the overall level of security may result in a reduction in functionality or usability. You should be cautious when applying these configurations to avoid interruption of required services.

TABLE OF CONTENTS

This document makes frequent references to the Data ONTAP documentation. This documentation is available on the NetApp Web site at *http://now.netapp.com/NOW/knowledge/docs/ontap/ontap_index.shtml.*

This document also refers to NetApp Technical Reports, which are available in the NetApp Library at *http://www.netapp.com/us/library/technical-reports/*.

1 DESIGNING A SECURE STORAGE INSTALLATION

1.1 NETWORK ASSESSMENT

Before designing or installing a NetApp storage system, you should perform a complete network assessment. A good network assessment looks at all parts of the proposed storage system, from physical cabling to protocols to current policies. The goal of the assessment is to provide detailed documentation to the design phase of the storage system. This is even more important when the storage system is being put into an existing network environment that was not designed with a storage system in mind.

INTERFACES

You should document all physical interfaces, including Ethernet switch ports, Fibre Channel switch ports, patch panels, and out-of-band management ports (such as terminal servers) in the areas where the storage network is proposed.

It is equally important to capture information on any logical interfaces already in use. This means documenting existing VLANs and Fibre Channel zones. Any gaps between physical port security and VLAN assignment need to be noted as part of the assessment.

SERVERS AND DATA

You should capture information on all existing servers in the network, including which servers are already exporting data, as well as applications and current data storage. Also note any server or storage virtualization solutions, and track LUN masking in Fibre Channel or iSCSI attached servers.

When documenting servers that are exporting data, also capture what types of data are exported. This will aid in a later phase when you document who accesses that data. Also document any encryption solutions in use, including encryption of data at rest and encryption of data transmission.

PROTOCOLS

In conjunction with the server assessment, you should make a complete list of current storage protocols. It's a good idea to note which protocols are in use on each server. Be sure to document thoroughly any areas where there are mixed-mode storage networks, such as requirements for NFS and CIFS shared home directories. List all iSCSI and Fibre Channel storage networks.

EXISTING ACCESS

This is probably the most complicated and data-intensive part of a network assessment. Determining who has access to what data, and for which reasons, can take a good deal of time and effort. However, this is your best opportunity to capture important data before beginning the design phase.

You should document three main categories of access here. First, capture the client access to mission-critical (business continuity) data, sensitive and personal data, home directories, and applications. In conjunction with listing the interfaces in the previous section, document the subnets or IP ranges that have access to networks on which critical data resides. A comprehensive understanding of how client access is authenticated needs to be part of this category. You should also note current security policies and key personnel.

Second, document the management access in use. Note local access, including serial ports and terminal servers. Capture any remote access methods here, whether they are CLI, Web, or application based. Clear documentation of how management access is authenticated is very important.

Finally, gather information on security policies that affect administration and management of existing systems. Include a list of key personnel who will be involved as the design phase progresses.

1.2 SECURE STORAGE DESIGN

With the network assessment completed, you have the information necessary to begin planning a secure storage installation. The assessment may have highlighted areas that need improvement or upgrade in order for the NetApp storage system to be as secure as possible.

Consider each of the following sections in your storage design.

PHYSICAL ACCESS

Any secure storage design considers physical access to all areas of the network. This is your opportunity to remedy any problems discovered in the network assessment. Consider access controls to the physical location of cabling, switches, servers, and storage hardware. Implement access controls for significant events such as connecting new switches, servers, and storage to a live storage network.

MANAGEMENT ACCESS

Do not default to allowing administrative access from “anywhere.” Plan a limited set of management networks and allow administrative access only from those networks. If there are servers or clients on these networks, limit administrative access from only those hosts that are necessary.

Data ONTAP has a wide set of features that enable limiting administrative access by network, host, or server, as well as the ability to restrict the roles that are allowed to administrators. Restrictions to administrative access can be granted to certain types of authenticated users and groups. The root user can also be completely disabled to further restrict administration.

NetApp recommends planning ahead for the secure administration of data storage. Data ONTAP allows SSH remote access as well as SSL-protected Web-based administration. NetApp strongly recommends these for use in all storage designs. Although Data ONTAP supports legacy clear-text protocols like telnet, NetApp does not recommend their use and they should be disabled wherever possible. Clear-text administrative protocols send passwords and commands in the clear and are not considered secure.

LOGICAL DESIGN

Although VLANs are not designed as a security feature, they provide an additional element of data separation that is important to consider. Where possible, you should use VLANs to separate management and client access, as well as to separate different classes of client access. You can enhance secure design by separating client and management access on different Ethernet ports.

You should also consider virtualization solutions here. MultiStore®, a licensed feature of Data ONTAP, is a storage virtualization solution that can provide increased security while allowing consolidation of storage. MultiStore can partition a NetApp storage system into secure logical containers that have their own storage, authentication, and management access. Combined with VLANs, this is a very powerful way to segregate data as needed.

You should also consider server virtualization solutions. Many virtual servers can share the same hardware, so it is important to carefully design the data paths from these virtual servers to the NetApp storage system. Again, taking advantage of VLANs and MultiStore helps separate data access in a secure fashion.

In storage networks, use Fibre Channel zoning to limit access in switches, servers, and storage devices. Use hardware-enforced zoning for additional access control. Use LUN masking at the point closest to the source device, as well as for iSCSI initiators. iSCSI interface access lists provide another layer of security for iSCSI initiators.

In multiprotocol IP networks, consider the use of permissions to further logically separate data. You can set NFS and CIFS permissions so that users of an NFS export cannot read the files in a CIFS export, even though the data physically resides in the same volume on the NetApp storage system.

PROTOCOL CONSIDERATIONS

The network assessment can provide useful data in this phase of secure storage design. Because the storage protocols already in use are documented, the system can be planned to include only necessary protocols. For example, it's not necessary to enable NFS and CIFS together on a storage network that requires only NFS access.

Make sure to avoid common errors. Restrict NFS exports to authorized users, with minimum required privileges. Do not grant root or administrator access to files exported by using NFS or CIFS. Disable client protocols on interfaces where they are not needed.

NetApp recommends the use of security features in IP storage protocols to secure client access:

- Employ strong user-level authentication by using Kerberos with NFS or CIFS.
- Use LDAP over SSL for centralized authentication and authorization.
- Enable LDAP signing and sealing with SASL.
- Enable CIFS signing to ensure the integrity of CIFS data transmission.
- Set CIFS authentication levels to accept only Kerberos authentication.
- Use NFSv4 whenever possible and limit NFSv3 usage.
- Enable NFSv4 ACLs and make sure that those ACLs are designed and assigned correctly.

CLIENT ACCESS

Designing for secure client access to storage can be time consuming and difficult. A thorough collection of client access requirements in the network assessment is invaluable in creating a secure storage design.

If you employ strong user-level authentication, you should also investigate encryption of data. You can use IPSec to protect data in transit, and use NetApp DataFort devices to encrypt data at rest.

Ensure that users have unique user IDs and that those IDs can be traced back to a specific user. Make sure that event logging is configured so that there is sufficient data to clearly identify users if necessary. Where possible, consider granting rights and privileges based on roles.

You should tightly conform with current security policies in the design. Try to avoid creating new security policies or roles. Data ONTAP has many methods to integrate authentication and authorization with existing protocols, which avoids the need to create unique user IDs for management of NetApp storage systems.

When you are creating volumes and qtrees for data management, NetApp strongly recommends that you organize data by security requirements. For example, if the NetApp storage system will store data for two groups (such as the finance and engineering departments in a company) with different access controls, place each data set on a separate volume to make security configuration simpler.

The most important documentation for this process is in the *Data ONTAP Storage Management Guide,* chapter 6, “Volume Management” and chapter 7, "Qtree Management."

2 INSTALLATION AND CONFIGURATION

This section describes specific settings and option values that you can use to configure a NetApp storage system in the most secure fashion possible.

Note: Many of these settings are set by default to the most secure value. The complete list is provided to assist you in auditing systems that have already been deployed.

2.1 ENABLE SECURE ACCESS

NetApp recommends that you configure and enable SecureAdmin™ immediately after initially setting up Data ONTAP. This best practice enables SSH and SSL encryption for secure administration of the NetApp storage system. Additional recommendations include using only the SSH version 2 protocol and using SSH public key authentication. For more information on SecureAdmin, see the *Data ONTAP System Administration Guide*, chapter 9, "Using SecureAdmin."

Although SSH version 1 is supported in Data ONTAP, it has known exploitable vulnerabilities that can be prevented only by using SSH version 2 exclusively. SSH public keys provide a stronger and more granular method of SSH access to NetApp storage systems.

SECUREADMIN	
Description	Enables SSH and SSL security features.
Recommended Setting	Use SecureAdmin to enable SSH and SSL.

Procedure	`toaster#` **`secureadmin setup –f ssh`**
	`toaster#` **`secureadmin enable ssh`**
	`toaster#` **`secureadmin setup ssl`**
	`toaster#` **`secureadmin enable ssl`**

HTTPS ADMINISTRATION	
Description	Enables/disables HTTPS administrative access to the NetApp storage system.
Recommended Setting	Enable HTTPS administrative access. Also use protocol access filters (see section 2.8) to restrict HTTPS administrative access.
Procedure	`toaster#` **`options httpd.admin.ssl.enable on`**
SSH VERSION 1	
Description	Enables/disables SSH version 1.
Recommended Setting	Disable SSH version 1.
Procedure	`toaster#` **`options ssh1.enable off`**
SSH VERSION 2	
Description	Enables/disables SSH version 2.
Recommended Setting	Enable SSH version 2.
Procedure	`toaster#` **`options ssh2.enable on`**
SSH PUBLIC KEY AUTHENTICATION	
Description	Enables/disables SSH public key authentication.
Recommended Setting	Enable SSH public key authentication.
Procedure	`toaster#` **`options ssh.pubkey_auth.enable on`**

2.2 DISABLE INSECURE AND UNNEEDED PROTOCOLS

Based on the network assessment from section 1, disable any unneeded and insecure protocols. Passing root or administrator passwords in clear text is not a best practice and should be avoided.

There are caveats to disabling some of these protocols. Data ONTAP FilerView® requires that **`httpd.admin.enable`** or **`http.admin.ssl.enable`** be set to "on." If the NetApp storage system is managed by using Operations Manager (formerly DataFabric® Manager), SNMP must be enabled. When enabling SNMP, choose a community string that is difficult to guess for all the SNMP-managed objects.

TRUSTED HOSTS ACCESS	
Description	Enables/disables the ability of certain hosts to access NetApp storage systems without authentication.
Recommended Setting	Disable the trusted host option.
Procedure	`toaster# options trusted.hosts -`
TELNET ACCESS	
Description	Enables/disables telnet access to the NetApp storage system.
Recommended Setting	Disable telnet access.
Procedure	`toaster# options telnet.enable off`
RSH ACCESS	
Description	Enables/disables RSH access to the NetApp storage system.
Recommended Setting	Disable RSH access.
Procedure	`toaster# options rsh.enable off`
HTTP ACCESS	
Description	Enables/disables HTTP access to the NetApp storage system.
Recommended Setting	Disable HTTP access. Alternatively, use protocol access filters (see section 2.8) to restrict HTTP access.
Procedure	`toaster# options httpd.enable off`
WEBDAV ACCESS	
Description	Enables/disables WebDAV access to the NetApp storage system.
Recommended Setting	Disable WebDAV access.
Procedure	`toaster# options webdav.enable off`
HTTP ADMINISTRATION	
Description	Enables/disables HTTP administrative access to the NetApp storage system.
Recommended Setting	Disable HTTP administrative access. Alternatively, use HTTP admin access (below) or protocol access filters (see section 2.8) to restrict HTTP administrative access.
Procedure	`toaster# options httpd.admin.enable off`
HTTP ADMIN ACCESS	
Description	Restricts HTTP administrative access to the NetApp storage system.
Recommended Setting	Restrict HTTP administrative access to specific hosts.
Procedure	`toaster# options httpd.admin.access host=[specific admin hosts]`
HOSTS.EQUIV ACCESS	
Description	File containing trusted remote hosts for HTTP administrative access without authentication.
Recommended Setting	Disable hosts.equiv access.
Procedure	`toaster# options httpd.admin.hostsequiv.enable off`

FTP	
Description	Enables/disables FTP.
Recommended Setting	Disable FTP access.
Procedure	`toaster# options ftpd.enable off`

PCNFS	
Description	Enables/disables PCNFS.
Recommended Setting	Disable PCNFS.
Procedure	`toaster# options pcnfs.enable off`

SNMP	
Description	Enables/disables SNMP.
Recommended Setting	Disable SNMP. If SNMP is required for management of the NetApp storage system, use protocol access filters (see section 2.8) to restrict SNMP access.
Procedure	`toaster# options snmp.enable off`

TFTP	
Description	Enables/disables TFTP.
Recommended Setting	Disable TFTP.
Procedure	`toaster# options tftpd.enable off`

NIS	
Description	Enables/disables NIS.
Recommended Setting	Disable NIS.
Procedure	`toaster# options nis.enable off`

2.3 PASSWORD SECURITY

Because the security of a NetApp storage system depends on limiting access to authorized administrators, it is *extremely important* that you select and manage administrator passwords very carefully. Use great caution to ensure that administrator passwords are difficult to guess. Don’t use words that are found in any dictionary or wordlist, including names, dates, place names, social security or other identifying numbers. Passwords should contain a mix of uppercase and lowercase letters, numbers, and nonalphanumeric characters.

Data ONTAP has many password options which you can set. The first option that you should always enable is **`security.passwd.rules.everyone`**, which forces all users on the storage system to conform to the same password rules. NetApp also recommends that you set the options for minimum password length; number of alphabetic, numeric, and symbols required; and the number of password attempts allowed before a user is locked out. These options are not substitutes for a strong password selection policy and administrator training on correct password selection.

ROOT PASSWORD	
Description	Sets the password for the root account.
Recommended Setting	Use a strong password for the root account.
Procedure	`toaster# passwd root [password]`

PASSWORD CHANGE	
Description	Requires all new administrative users to change their password at first login.
Recommended Setting	Enable password change.
Procedure	`toaster# options security.passwd.firstlogin.enable on`

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	toaster# **options security.passwd.rules.enable on**

PASSWORD RULES	
Description	Applies password rules to all users on the NetApp storage system.
Recommended Setting	Enable password rules.
Procedure	toaster# **options security.passwd.rules.everyone on**

PASSWORD LOCKOUT	
Description	Locks out administrative user accounts after a set number of incorrect passwords are entered.
Recommended Setting	Enable password lockout. Choose a number of attempts less than 6; or set to comply with corporate security policy. The root user is not affected by this option, and cannot be locked out.
Procedure	toaster# **options security.passwd.lockout.numtries 6**

PASSWORD HISTORY	
Description	Controls whether an administrator can use a previous password.
Recommended Setting	Enable password history. Choose a number of passwords greater than 6; or set to comply with corporate security policy.
Procedure	toaster# **options security.passwd.rules.history 6**

PASSWORD MAXIMUM LENGTH	
Description	Controls the maximum length of administrator passwords.
Recommended Setting	Set password maximum length. Choose a maximum size password of 14; or set to comply with corporate security policy. Passwords longer than 14 characters are not supported with Windows® administrative interfaces.
Procedure	toaster# **options security.passwd.rules.maximum 14**

PASSWORD MINIMUM LENGTH	
Description	Controls the minimum length of administrator passwords.
Recommended Setting	Set password minimum length. Choose a minimum size password of 8; or set to comply with corporate security policy.
Procedure	toaster# **options security.passwd.rules.maximum 8**

PASSWORD MINIMUM ALPHABETIC	
Description	Controls the minimum number of alphabetic characters in administrator passwords.
Recommended Setting	Set password minimum alphabetic length. Choose a minimum size of 6; or set to comply with corporate security policy.
Procedure	toaster# **options security.passwd.rules.minimum.alphabetic 6**

PASSWORD MINIMUM DIGIT	
Description	Controls the minimum number of numeric characters in administrator passwords.
Recommended Setting	Set password minimum numeric length. Choose a minimum size of 1; or set to comply with corporate security policy.
Procedure	toaster# **options security.passwd.rules.minimum.digit 1**

PASSWORD MINIMUM SYMBOL	
Description	Controls the minimum number of nonalphanumeric characters in administrator passwords.
Recommended Setting	Set password minimum nonalphanumeric length. Choose a minimum size of 1; or set to comply with corporate security policy.
Procedure	toaster# **options security.passwd.rules.minimum.symbol 1**

2.4 AUTOLOGOUT

You should enable autologout for console and telnet (if enabled) sessions and set autologout timeouts to comply with security policies. If SSH is enabled, you should also set the SSH idle timeout.

Note: If you are using the NetApp Remote LAN Management (RLM) card, these options are ignored when accessing the NetApp storage system using the RLM. See the *Data ONTAP System Administration Guide* for details.

AUTOMATIC LOGOUT	
Description	Enables and sets an automatic logout for idle console and telnet sessions to the NetApp storage system.
Recommended Setting	Enable automatic logout. Choose a length of 5 minutes; or set to comply with corporate security policy.
Procedure	toaster# **options autologout.console.enable on** toaster# **options autologout.telnet.enable on** toaster# **options autologout.console.timeout 5** toaster# **options autologout.telnet.timeout 5**
SSH IDLE TIMEOUT	
Description	Enables and sets an automatic timeout for idle SSH sessions to the NetApp storage system.
Recommended Setting	Enable automatic timeout. Choose a length of 10 minutes (600 seconds) or set to comply with corporate security policy.
Procedure	toaster# **options ssh.idle.timeout 600**

2.5 LOGGING

Audit logging should always be enabled. This logs administrative access from the console and from remote shell sessions. Log file size depends on corporate security policy, but it should be large enough to record several days' worth of administrative usage at a minimum. A best practice is to set log file size to a large value (several megabytes, at least) and then adjust the size after monitoring growth of the log file.

Some corporate security policies may dictate central log collection and analysis. Data ONTAP does support the sending of audit logs to an external syslog host. Although NetApp does not recommend external syslog as a best practice, consider this option as a way to collect historical data, particularly if you have enabled CIFS or NFS logging, as discussed in sections 4.1 and 4.2. See the man page for **`syslog.conf`** for details.

LOGGING ADMINISTRATIVE ACCESS	
Description	Enables and configures logging for administrative sessions.
Recommended Setting	Enable logging for administrative sessions.
Procedure	toaster# **options auditlog.enable on** toaster# **options auditlog.max_file_size [logfilesize]**

2.6 NETWORK AND IP OPTIONS

Because NFS, CIFS, iSCSI, and administrative clients access Data ONTAP over TCP/IP networks, it is important to configure the networking on the NetApp storage system in a secure fashion. The most relevant documentation for this purpose is the *Data ONTAP Network Management Guide.*

You can set many IP options in Data ONTAP. Routed is enabled by default, but it is not needed in many enterprise networks and can be turned off. Disable IP fastpath to remove the possibility of ARP spoofing attacks. Enable packet checking to verify source IP addresses.

INCOMING PACKETS	
Description	Checks incoming packets for correct addressing. If this option is on, the NetApp storage system accepts any packet that is addressed to it, even if that packet came in on the wrong interface.
Recommended Setting	Enable packet checking for correct addressing.
Procedure	`toaster#` **`options ip.match_any_ifaddr off`**
MAC FASTPATH	
Description	The NetApp storage system attempts to use MAC address and interface caching (fastpath) to try to send back responses to incoming network traffic by 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, increases the ability for ARP spoofing and session hijacking attacks.
Procedure	`toaster#` **`options ip.fastpath.enable off`**
PING FLOOD	
Description	Specifies the maximum number of ICMP echo or echo reply packets that Data ONTAP accepts per second. Any further packets within 1 second are dropped to prevent ping flood denial of service attacks..
Recommended Setting	Enable ping flood protection.
Procedure	`toaster#` **`options ip.ping_throttle.drop_level 150`**
LOGGING PING FLOOD	
Description	Specifies how often dropped pings are logged, in minutes. This prevents a ping flood denial of service attack from flooding the audit log with messages.
Recommended Setting	Enable logging of ping attacks.
Procedure	`toaster#` **`options ip.ping_throttle.alarm_interval 5`**
ROUTED	
Description	Enables/disables the internal routed process in Data ONTAP. Routed enables IDRP router discovery and listening for RIP packets. You can safely disable routed if you do not rely on IRDP or RIP for routing updates. **Note:** Enabling the MultiStore license in Data ONTAP automatically disables the routed process.
Recommended Setting	Disable routed. **Note:** If the command-line option is used to disable routed, after a system reboot routed will be reenabled. You can permanently disable routed in the Network section of FilerView (HTTP administration).
Procedure	`toaster#` **`routed off`**

2.7 OTHER PROTOCOL OPTIONS

Regardless of the types of data stored on the system or which methods are used to access that data, you must perform backups to protect the data in case of a system failure or other disaster. Data ONTAP provides several methods (SnapMirror®, SnapVault®, and NDMP) that you can use to perform backups over a TCP/IP network. This kind of network backup has security considerations that you must address. The *Data Protection Online Backup and Recovery Guide* provides information about how to configure security for these kinds of backups, as well as information on network-based NDMP tape backups.

NetApp recommends that you enable SnapMirror source access verification. If NDMP is in use, MD5 authentication is also a best practice.

SNAPMIRROR SOURCE ACCESS	
Description	Enables IP address-based verification of SnapMirror destination NetApp storage systems by source NetApp storage systems.
Recommended Setting	Enable source address verification.
Procedure	`toaster#` **`options snapmirror.checkip.enable on`**
NDMP AUTHENTICATION	
Description	Sets the NDMP authentication type.
Recommended Setting	Enable MD5 authentication for NDMP.
Procedure	`toaster#` **`options ndmpd.authtype challenge`**

2.8 PROTOCOL ACCESS CONTROLS

Data ONTAP has two sets of options that you can use to control protocol access to a FAS storage system. NetApp recommends that you use both of these options in all environments where restriction of protocol access is needed.

PROTOCOL BLOCKING

Introduced in Data ONTAP 7.3, protocol blocking enables you to specifically disable several protocols by physical interface, providing additional flexibility when designing secure storage systems. For example, NFS could be blocked on a pair of interfaces, so that NFS requests to either of these interfaces are ignored.

PROTOCOL BLOC KING	
Description	Sets a comma-separated list of interface names for which a specific protocol is blocked. To disable blocking for a protocol, use an empty set of "".
Recommended Setting	Enable protocol blocking in any situation where access controls for client protocols are needed.

Procedure	`toaster#` **`options interface.blocked.cifs e5b`**
	`toaster#` **`options interface.blocked.nfs e1a,e1b`**
	`toaster#` **`options interface.blocked.iscsi e5b`**
	`toaster#` **`options interface.blocked.ftpd e5b,e1a,e1b`**
	`toaster#` **`options interface.blocked.snapmirror e4a,e4b`**
	`toaster#` **`options interface.blocked.cifs “”`**

PROTOCOL ACCESS FILTER

Data ONTAP allows the configuration of filters for the following protocols: RSH, telnet, SSH, HTTP, SNMP, NDMP, SnapMirror, and SnapVault. For a detailed description of usage, refer to the man page for **`na_protocolaccess`**.

The filters can specify hostnames, IP addresses, IP subnets, or interface names, which are either allowed or disallowed for each protocol. Each application then uses the filter on the listening socket to control access.

In conjunction with disabling insecure protocols, this allows a fine-grained control of access from limited areas. NetApp recommends as a best practice that you configure protocol access filters for any administrative protocol that is enabled on the NetApp storage system.

The following table shows some protocol access control examples.

Description	Allow remote shell access for only one host, named gnesha.
Command	**`options rsh.access "host = gnesha"`**
Description	Allow telnet access for subnet 10.42.69.0.
Command	**`options telnet.access host=10.42.69.0/24`**
Description	Allow SSH access for hosts abc and xyz when on network interface e0.
Command	**`options ssh.access "host=abc,xyz AND if=e0"`**
Description	Allow SNMP access for network interfaces e0, e1, and e2.
Command	**`options snmp.access “if=e0,e1,e2”`**
Description	Do not allow access to HTTPD for network interface e3.
Command	**`options httpd.access "if != e3"`**
Description	Allow administrative HTTPD access for hosts champagne and tequila.
Command	**`options httpd.admin.access “host=champagne,tequila”`**
Description	Disallow all access to telnet.
Command	**`options telnet.access "host=-"`**
Description	Use **`/etc/snapmirror.allow`** to check access to SnapMirror sources.
Command	**`options snapmirror.access legacy`**
Description	Allow a SnapVault server to accept any client requests.
Command	**`options snapvault.access all`**
Description	Allow an NDMP server to accept a connection request from a single backup server.
Command	**`options ndmpd.access ”host = backup”`**

3 ADMINISTRATIVE ACCESS

It is important to note that the "users" described in the *Data ONTAP System Administration Guide* are local and should be created and used only for system administrators *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."

Data ONTAP supports several methods of creating and managing administrative users. Local users can be defined and managed on each NetApp storage system. Windows users can use their Active Directory® credentials to manage Data ONTAP. Role-based access control (RBAC) provides powerful limits for administrative separation. Finally, centralized administration allows use of NIS and LDAP authentication for administrative users.

3.1 LOCAL AND DOMAIN USERS

As a best practice, administrative users should be created in Active Directory, NIS, or LDAP environments when these methods of authentication are available. Maintaining separate administrative users on the NetApp storage system is supported. However, the flexibility of external authentication combined with the ability to easily support local security policies means that you should consider any of these other forms of authentication before creating local administrative accounts. NetApp recommends that you disable the local root user account when other administrative accounts are in use.

NONROOT USERS	
Description	Creates additional accounts on the NetApp storage system.
Recommended Setting	Create nonroot user accounts for each administrator.
Procedure	`toaster#` **`useradmin useradd [username]`**
WINDOWS DOMAIN USERS	
Description	Adds Windows domain users to the administrator list for the NetApp storage system. This enables you to use existing Active Directory authentication and groups to manage Data ONTAP without creating local user accounts on each NetApp storage system.
Recommended Setting	In Windows environments, create domain user accounts for each administrator.
DISABLE ROOT USER	
Description	Disables the local root user account. This option must be set by a nonroot administrative user who has the `security-complete-user-control` capability defined. To reset the option and enable root access, a nonroot administrative user must first change the root password.
Recommended Setting	Disable the local root user account only when other administrative accounts have been created with sufficient privileges to manage Data ONTAP.
Procedure	`toaster#` **`options security.passwd.rootaccess.enable off`**

3.2 CENTRALIZED ADMINISTRATION

A new feature added in Data ONTAP 7.2 allows administrative users to be defined from NIS or LDAP external authentication. As with Windows domain users, this reduces the need to have local users and passwords defined on the NetApp storage system. Administrative users are then compliant with established security policies for user names, passwords, and groups.

You can combine this flexibility with RBAC to limit all aspects of administration in Data ONTAP. One caveat is that only a single NIS or LDAP group is allowed to participate in administration of the NetApp storage system.

To configure centralized administration, you must set the following options.

ADMINISTRATIVE AUTHENTICATION	
Description	Controls where Data ONTAP finds authentication information for administrative users.
Recommended Setting	Enable nsswitch authentication, allowing NIS or LDAP authentication. Allow secondary authentication from internal Data ONTAP users.
Procedure	`toaster#` **`options security.admin.authentication nsswitch,internal`**
ADMINISTRATIVE GROUP	
Description	Specifies the administrative group from the authentication method set in `/etc/nsswitch.conf` on the NetApp storage system. This option must be set to a valid NIS or LDAP group.
Recommended Setting	Define the appropriate administrative group from an NIS domain or LDAP.
Procedure	`toaster#` **`options security.admin.nsswitchgroup [groupname]`**

Additionally, the **`/etc/nsswitch.conf`** file on the NetApp storage system needs to be edited. The following example supports LDAP, NIS, and local authentication:

```
toaster# rdfile /etc/nsswitch.conf
passwd: ldap nis files
group: ldap nis files
netgroup: ldap nis files
```

For more information on configuring LDAP for NetApp storage systems, see the NetApp technical report TR-3458..

3.3 ROLE-BASED ACCESS CONTROL

RBAC is a method for managing the set of actions that an administrator can perform on the NetApp storage system. Instead of issuing root access to all of the storage administrators who need access to Data ONTAP; you can make available only the level of access that is required for a job function.

There are four parts to RBAC in Data ONTAP.

USERS

An RBAC *user* is defined as an account that is authenticated on the NetApp storage system. This can be a local user, a Windows domain user, or a user in a specific NIS or LDAP group. Normal users who access data stored on the NetApp storage system are not part of this definition.

GROUPS

A *group* is simply a collection of RBAC users. Groups are assigned one or more roles. Groups defined in Data ONTAP are separate from Windows, NIS, or LDAP groups; they are defined specifically for the purposes of assigning roles to their users.

When you create new users or Windows domain users, Data ONTAP requires that you specify a group membership. It is a best practice to create appropriate groups before creating local users or Windows domain users.

ROLES

Roles are defined as sets of capabilities. Data ONTAP comes with several predefined roles, which you can modify. You can also create new roles. Again, when you create new groups, Data ONTAP requires that you specify roles for the new groups. It is a best practice to create appropriate roles before creating groups or users.

CAPABILITIES

A *capability* is defined as the privilege granted to a role to execute commands or take other specified actions. Data ONTAP uses four types of capabilities:

- Login rights: These capabilities have names that begin with “login-“ and are used to control which access methods an administrator is permitted to use for managing the system.
- CLI rights: These capabilities have names that begin with “cli-“ and are used to control which commands an administrator can use in the Data ONTAP command-line interface.
- API rights: These capabilities have names that begin with “api-“ and are used to control which application programming interface (API) commands you can used. API commands are usually executed by programs, rather than directly by administrators.
- Security rights: These capabilities have names that begin with “security-“ and are used to control the ability to use advanced commands or to change passwords for other users.

You should thoroughly plan a complete RBAC implementation before execution. For additional information on role-based access control in Data ONTAP, refer to the NetApp technical report TR-3358.

4 CLIENT ACCESS

When you use Data ONTAP for file access, there are two realms of security to manage. One realm is the security of the NetApp storage system running Data ONTAP, including security controls on exported file systems (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 by using the **chown** and **chmod** UNIX® commands or from CIFS clients by using the procedures in the "Changing and displaying file-level ACLs" and "Changing UNIX permissions and DOS attributes from Windows" sections of the *Data ONTAP File Access Management Guide.*

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 to follow in setting access controls and permissions on files and directories. Even if the NetApp storage 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 can inadvertently compromise the security of the data in that file. You must implement programs to ensure constant awareness and education of individual nonadministrative users on local security policy.

Data ONTAP supports many security options for NAS protocols. In addition, the multiprotocol capabilities of Data ONTAP mean that there are best practices that you should follow in mixed CIFS/NFS environments.

4.1 CIFS

Chapter 10, "Virus Protection for CIFS," in the *Data ONTAP Data Protection Online Backup and Recovery Guide* contains information on how to provide virus scanning services for files accessed by using CIFS. This functionality requires a third-party antivirus scanner system from McAfee, Computer Associates, Symantec, or Trend Micro. NetApp strongly recommends that all customers who use CIFS deploy an antivirus server. For more about antivirus best practices, see the NetApp technical report TR-3107.

NetApp recommends the following best practices to securely implement CIFS:

- Active Directory authentication using Kerberos
- LDAP signing and sealing with SASL and LDAP transport over SSL
- CIFS signing to ensure integrity of CIFS traffic
- Storage-Level Access Guard to provide a third layer of security to CIFS and NFS
- CIFS auditing to provide very granular logging information

KERBEROS AUTHENTICATION	
Description	Active Directory 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. See the NetApp technical report TR-3457 for more information on setting up NetApp storage systems with Active Directory authentication by using Kerberos.
UNIFIED LDAP AUTHORIZATION	
Description	Enables Active Directory LDAP for user authorization with CIFS and NFS clients.
Recommended Setting	Use Active Directory LDAP in any environment where Active Directory is the primary LDAP store.
Procedure	See the NetApp technical report TR-3458 for more information on setting up NetApp storage systems with Active Directory authentication using Kerberos to support CIFS and NFS clients.

LDAP SECURITY LEVEL	
Description	In conjunction with setting up LDAP for authentication and authorization, LDAP signing provides another level of security, and LDAP sealing provides encryption of all LDAP packets.
Recommended Setting	Enable LDAP signing and sealing with SASL. Enable LDAP over SSL.
Procedure	`toaster#` **`options ldap.security.level 2`**
CIFS SIGNING	
Description	Enables CIFS signing to ensure the integrity of CIFS communications.
Recommended Setting	Ensure that CIFS signing is enabled on both the NetApp storage system and the Windows clients.
Procedure	On the NetApp storage system: `toaster#` **`options cifs.signing.enable on`** On the Windows client: Enable **`EnableSecuritySignature`** and **`RequreSecuritySignature`** parameters in the Windows registry: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SeCEdit\Reg Values\MACHINE/System/CurrentControlSet/Services/LanManServer/Parameters/EnableSecuritySignature HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SeCEdit\Reg Values\MACHINE/System/CurrentControlSet/Services/LanManServer/Parameters/RequireSecuritySignature
SESSION AUTHENTICATION LEVEL	
Description	Determines which challenge/response authentication protocol is used for Windows net logon. The following levels of authentication are supported: • 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
Recommended Setting	For the highest session authentication level, set this option to 5 to accept only Kerberos authentication. Setting the option to this level supports only Windows 2000 and later versions of Windows.
Procedure	`toaster#` **`options cifs.LMCompatibilityLevel 5`**
SHARE-LEVEL PERMISSIONS	
Description	Sets the share-level permission on the NetApp storage system CIFS shares.
Recommended Setting	Change the share-level ACL to authorized users only and remove Everyone/Full Control.
Procedure	`toaster#` **`cifs access <sharename> [-g] <user|group> <rights>`**
ACCESS-BASED ENUMERATION	
Description	Data ONTAP 7.2 and later releases provide storage system support for Access-Based Enumeration (ABE), a shared resource security feature introduced in Microsoft Windows Server 2003 Service Pack 1. 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.
Recommended Setting	Enable ABE on CIFS shares in Windows Server 2003 SP1 environments. See the NetApp technical report TR-3367 for more information on Access-Based Enumeration.
Procedure	`toaster#` **`cifs access <sharename> <–accessbasedenum>`**
ANONYMOUS CONNECTIONS (RESTRICT ANONYMOUS)	
Description	Controls access to users with nonauthenticated connections. Permitted values for this option are 0, 1, and 2. 0 sets no special access restrictions, 1 disallows enumeration of users and shares, and 2 fully restricts access. This option corresponds to the RestrictAnonymous registry entry in Windows.
Recommended Setting	Disable access to CIFS shares and sharenames from unauthenticated users.
Procedure	`toaster#` **`options cifs.restrict_anonymous 2`**

GUEST ACCESS	
Description	Enables/disables CIFS guest access.
Recommended Setting	Disable CIFS guest access.
Procedure	toaster# **options cifs.guest_account “”**

STORAGE-LEVEL ACCESS GUARD	
Description	In Data ONTAP 7.2.2 and later, creates a third level of access control for CIFS and NFS shares.
Recommended Setting	Enable Storage-Level Access Guard. See the NetApp technical report TR-3596 for more information on enabling and configuring Storage-Level Access Guard.
Procedure	toaster# **fsecurity apply <definition file path> [<options>]**

GROUP POLICY OBJECTS	
Description	A Group Policy Object (GPO) is a set of rules that are applicable to users and computers in an Active Directory environment and defined centrally for ease of administration and increased security. Data ONTAP is able to recognize and process a certain set of GPOs.
Recommended Setting	Enable GPO support. Use GPO for file system security, restricted security groups, event login, and audit policy mapping. See the NetApp technical report TR-3367 for more information on Group Policy Objects.
Procedure	toaster# **options cifs.gpo.enable on**

WINDOWS DOMAIN MACHINE PASSWORD	
Description	By default, a NetApp storage system in a Windows 2000 domain does not automatically change its machine password. This option enables you to change the machine password weekly.
Recommended Setting	Enable weekly changes of the machine password.
Procedure	toaster# **options cifs.weekly_W2K_password_change on**

NETBIOS OVER TCP	
Description	Enables/disables NetBIOS transport over TCP. If disabled, legacy Windows clients and domains do not communicate with the NetApp storage system. This option takes effect when CIFS is started in Data ONTAP. It should not be changed while CIFS is enabled.
Recommended Setting	Disable NetBIOS over TCP.
Procedure	toaster# **options cifs.netbios_over_tcp.enable off**

AUDIT CIFS ACCESS	
Description	Audits CIFS access.
Recommended Setting	Enable the auditing of CIFS access to the NetApp storage system. See the NetApp technical report TR-3595 for information on auditing CIFS and NFS protocols with Data ONTAP.
Procedure	toaster# **options cifs.audit.enable on**

AUDIT CIFS ACCOUNT MANAGEMENT EVENTS	
Description	Audits CIFS file access events when a System Access Control List (SACL) matches a request for access.
Recommended Setting	Enable the auditing of CIFS file access events. See the NetApp technical report TR-3595 for information on auditing CIFS and NFS protocols with Data ONTAP.
Procedure	toaster# **options cifs.audit.account_mgmt_events.enable on**

AUDIT CIFS FILE ACCESS EVENTS	
Description	Audits CIFS account creation, deletion, and modification.
Recommended Setting	Enable the auditing of CIFS account management events. See the NetApp technical report TR-3595 for information on auditing CIFS and NFS protocols with Data ONTAP.
Procedure	toaster# **options cifs.audit.file_access_events.enable on**

AUDIT CIFS LOGON EVENTS	
Description	Audits CIFS logons and logoffs, including CIFS session connects and disconnects.
Recommended Setting	Enable the auditing of CIFS logon events. See the NetApp technical report TR-3595 for information on auditing CIFS and NFS protocols with Data ONTAP.
Procedure	toaster# **options cifs.audit.logon_events.enable on**

CIFS auditing can be a complex undertaking. In addition to a large volume of data being logged, there is the potential of performance degradation on the Windows hosts as well as the NetApp storage system. You should give careful consideration to which CIFS events are audited.

In addition, NetApp recommends the following best practices for CIFS auditing:

- Try to avoid Security Access Control Lists (SACLs) that contain "Full Control" for "Everyone"
- Minimize the number of entries in the SACL for an object
- To maximize the effectiveness of auditing, audit only the actions that are really interesting
- Set an appropriate size for the event log file

Microsoft publishes a best practices guide to auditing security events, available at *http://technet2.microsoft.com/windowsserver/en/library/5658fae8-985f-48cc-b1bf-bd47dc2109161033.mspx*.

4.2 NFS

NetApp recommends a number of best practices to securely deploy NFS:

- Kerberos authentication
- LDAP signing and sealing with SASL and LDAP transport over SSL
- Enable NFSv4
- Enable NFS over TCP
- Restrict NFS to low-numbered ports

KERBEROS AUTHENTICATION	
Description	Enables Kerberos authentication for NFS. Requires NFS clients to support Kerberos.
Recommended Setting	Enable NFS authentication with Kerberos. Refer to the NetApp technical report TR-3481 for information on setting up Kerberos with NetApp storage systems.
Procedure	`toaster#` **`nfs setup`** After performing the nfs setup command**,** edit **`/etc/exports`** on the NetApp storage system to set **`“sec=krb5”, “sec=krb5i”,`** or **`“sec=krb5p”`** in the options field of the exported file systems.

LDAP AUTHORIZATION	
Description	Enables LDAP directory lookup service for user authorization. SSL is also supported for secure connection.
Recommended Setting	Enable LDAP user lookup for authorization. Enable LDAP over SSL or SASL. Refer to the NetApp technical report TR-3464 for information on setting up LDAP with NetApp storage systems.

Procedure	`toaster#` **`options ldap.enable on`**
	`toaster#` **`options ldap.ssl.enable on`**

NFS VERSION 4	
Description	Enables NFS version 4, allowing use of NFSv4 Access Control Lists (ACLs).
Recommended Setting	Enable NFSv4. Where possible, disable NFSv3 at the same time. See the NetApp technical report TR-3580 for information on NFSv4.

Procedure	`toaster#` **`options nfs.v4.enable on`**
	`toaster#` **`options nfs.v4.acl.enable on`**

NFS OVER TCP	
Description	Enables NFS sessions by using TCP packets instead of UDP. 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 it is better practice to deploy the NFS clients and servers in the same security zone.
Recommended Setting	Enable NFS over TCP.
Procedure	toaster# **options nfs.tcp.enable on** toaster# **options nfs.udp.enable off**
NFS MOUNT REQUEST	
Description	Enables/disables NFS mount requests over high-numbered ports. Low-numbered ports are restricted to root users and are considered more secure.
Recommended Setting	Restrict NFS mounts to low-numbered ports only.
Procedure	toaster# **options nfs.mount_rootonly on**

THE /ETC/EXPORTS FILE

You can use the **man na_exports** command to get a complete description of all the available options for NFS export in Data ONTAP. This section describes the options related to security.

Access Rules

Make sure that you are using the appropriate security options in the NFS export to prevent unsolicited clients from mounting or gaining elevated access rights to the desired volumes on the NetApp storage system. In the following example, suppose that you want to grant read-write permission on volume **/vol/volx** to host1, grant read-only permission to host2, and no other hosts can mount the volume.

In Data ONTAP 6.5 and later, enter:

```
/vol/volx -rw=host1,ro=host2
```

Security-Related Export Options

The following NFS export options are related to security. Use these options appropriately to secure data in an NFS environment.

anon

This option specifies the effective user ID (or name) of all anonymous or root NFS client users that access the file system path. An anonymous NFS client user is an NFS client user that does not provide valid NFS credentials; a root NFS client user is an NFS client user with a user ID of 0. Data ONTAP determines a user's file access permissions by checking the user's effective user ID against the NFS server's **/etc/passwd** file. By default, the effective user ID of all anonymous and root NFS client users is 65534.

To disable root access by anonymous and root NFS client users, set the anon option to 65535. To grant root user access to all anonymous and root NFS client users, set the **anon** option to 0. This is equivalent to the **no_root_squash** option in some other NFS servers. If a name is provided instead of a user ID, that name is looked up according to the order specified in the /etc/nsswitch.conf file, which determines the corresponding user ID to be assigned by the anon option.

nosuid

This option disables the `setuid` and `setgid` executables and `mknod` commands on the file system path. Unless the file system is a root partition of a diskless NFS client, you should set the `nosuid` option to prevent NFS client users from creating `setuid` executables and device nodes that careless or cooperating NFS server users could use to gain root access.

sec

Starting with version 6.5, Data ONTAP supports the ability to specify multiple security (sec) options for each exported resource. The administrator can determine how secure NFS access is to the NetApp storage system. Basically, the following two security service types are supported.

- UNIX (AUTH_SYS) authentication (sys): Does not use strong cryptography and is the least secure of the security services. This is the default security service used by Data ONTAP.

  Note: AUTH_SYS credentials are basically a user ID and up to 17 group IDs. Once a person is logged in as a superuser on a UNIX system, that person can use the `su` command to become a user who is allowed full access to a volume. One way to prevent this scenario from happening is to implement strong authentication mechanisms such as Kerberos.
- Kerberos 5 Provides the following three security methods:
  - Authentication (**`krb5`**): Uses strong cryptography to prove a user's identity to a storage system and to prove a storage system's identity to a user.
  - Integrity (**`krb5i`**): Provides a cryptographic checksum of the data portion of each request and the response message to each request. This defends against "man in the middle" tampering with storage system NFS traffic.
  - Privacy (**`krb5p`**): Encrypts the contents of packets bidirectionally, including procedure arguments and user data, by using a shared session key established by the client from the storage system.

The following two examples show how these security services are used:

To specify one security type, enter:

```
/vol/volx –sec=sys,rw=host1
```

To specify multiple security types, enter:

```
/vol/volx –sec=krb5:krb5i:krb5p,rw=host1
```

For more information on setting up NFS using Kerberos authentication, refer to these NetApp technical reports:

- TR-3481 for a key distribution center (KDC) based on UNIX
- TR-3457 for a KDC based on Active Directory

4.3 ISCSI

For systems that are configured to provide LUN access by using iSCSI, read the *Block Access Management Guide*, especially chapter 6, "Managing iSCSI Initiator Groups." NetApp recommends several best practices to secure iSCSI storage:

- Enable iSCSI only on necessary interfaces
- Disable access for initiators with no security method
- Use CHAP authentication with random 128-bit passwords
- Use LUN masking to control access to specific initiators
- Use iSCSI interface access lists to restrict initiators to specific interfaces

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	toaster# **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	toaster# **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 information on generating a random 128-bit password.
Procedure	toaster# **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	toaster# **iscsi security generate**
LUN MASKING	
Description	Each iSCSI LUN can be restricted to a specified group of iSCSI initiators. NetApp refers to these initiators groups as *igroups*. This initiator-to-igroup to LUN combination is known as LUN masking.
Recommended Setting	Use LUN masking to restrict LUN access to specific igroups. Create an igroup, then create the LUN, and finally create the mask.
Procedure	toaster# **igroup create –i –t windows igroup-name [node-name]** toaster# **lun create –s size –t windows lun_name** toaster# **lun map lun_name igroup_name [lun_ID]**
INTERFACE ACCESS LISTS	
Description	Each iSCSI initiator can be restricted to specific network interfaces. This is particularly useful in VLAN environments, where an initiator may not be able to access all interfaces on the NetApp storage system. Creating or modifying an access list may cause sessions to be shut down, so use these commands carefully.
Recommended Setting	Use iSCSI interface access lists to control initiator access.
Procedure	toaster# **iscsi interface accesslist add [initiator] [-a interface]** toaster# **iscsi interface accesslist remove [initiator] [-a interface]** toaster# **iscsi interface accesslist show [-a]**

4.4 FIBRE CHANNEL

For systems that are configured to provide LUN access by using FCP, see the *Block Access Management Guide*, especially chapter 7, "Managing FCP Initiator Groups."

FCP security should be enhanced by implementing zoning restrictions on the Fibre Channel switch that may be deployed as part of the configuration; see the switch documentation 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.

4.5 MULTIPROTOCOL OPTIONS

Data ONTAP has several options that you should use in networks where CIFS and NFS are both in use.

IGNORE ACLS	
Description	When on, ACLs do not affect root access from NFS. The option defaults to off.
Recommended Setting	Disable the ignoring of any ACLs.
Procedure	toaster# **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	toaster# **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 requester is not the file owner. In all cases, Windows client requests are checked against the share-level ACL. If the requester is the owner, the "user" permissions are used to determine the access permissions. If the requester is not the owner, and if **cifs.perm_check_use_gid** is **on**, files with UNIX security are checked using normal UNIX rules; that is, if the requester is a member of the file's owning group, the "group" permissions are used; otherwise, the "other" permissions 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 against the file's "group" permissions, and the "other" permissions are ignored. In effect, the "group" permissions 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.
DEFAULT WINDOWS USER	
Description	Specifies the Windows domain user account to use when a UNIX user accesses a file with Windows 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 user mapping configured correctly; disabling this access on an NFS-only NetApp storage system results in access problems for legitimate users.
Procedure	toaster# **options wafl.default_nt_user “”**
DEFAULT UNIX USER	
Description	Specifies the UNIX user account to use when a Windows domain user attempts to log in and that Windows 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 user mapping configured correctly; disabling this access on a CIFS-only NetApp storage system results in access problems for legitimate users.
Procedure	toaster# **options wafl.default_unix_user “”**

ROOT TO ADMIN MAPPINGS	
Description	When on (the default), a Windows domain administrator is mapped to UNIX root.
Recommended Setting	Disable root to administrator mappings by default.
Procedure	`toaster# options wafl.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	`toaster# options wafl.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 20160.
Recommended Setting	Set the minutes for cache credentials to 10.
Procedure	`toaster# options wafl.wcc_minutes_valid 10`
PRESERVE UNIX SECURITY	
Description	Preserves UNIX permissions as files are edited and saved by Windows applications that use temporary files. Enabling this option allows UNIX file permissions to be set by using the Security tab on a Windows client. When enabled, this option causes UNIX qtrees to appear as NTFS volumes. This option affects only NFS files in UNIX or mixed-mode qtrees.
Recommended Setting	Enable this option if you are in a mixed UNIX and Windows environment where files are edited by cross-platform client applications.
Procedure	`toaster# cifs.preserve_unix_security on`
FILE POLICIES	
Description	File policies specify file operation permissions 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. FPolicy requires CIFS to be licensed and running, even in NFS-exclusive environments.
Recommended Setting	Enable file policies if required by corporate security policy.
Procedure	See the *Data ONTAP File Access and Protocols Management Guide* for more information on enabling file policies.

5 CONCLUSION

Secure storage is increasingly important as storage of business-critical data, personal data, and customer data increases exponentially. You can achieve a secure storage design with the data collected in a thorough network assessment. Following the design recommendations in this document assists you in creating a secure storage environment for NetApp storage systems.

Data ONTAP has many security-related options that should be properly set in a secure storage environment. Many of these options allow compliance with corporate security policies. NetApp strongly recommends that you use secure administration methods for Data ONTAP and that you disable any unsecure administrative protocols.

Client access to a secure storage system is vitally important. NetApp recommends the use of secure authentication and authorization in addition to the various protocol-dependent methods of secure data transfer.

www.netapp.com