Technical Report

Best Practices for Secure Configuration of Data ONTAP 7G

Ronald Demery CISSP, NetApp

February 2012 | TR-3649

ABSTRACT: UPDATED FOR DATA ONTAP 7.3.7

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 might 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

1 DESIGNING A SECURE STORAGE INSTALLATION 4

1.1 NETWORK ASSESSMENT 4

1.2 SECURE STORAGE DESIGN 5

2 INSTALLATION AND CONFIGURATION 7

2.1 ENABLE SECURE ADMINISTRATIVE ACCESS 7

2.2 DISABLE OR MODIFY DEFAULT ACCOUNTS 10

2.3 DISABLE UNNECESSARY SERVICES 13

2.4 PASSWORD SECURITY 13

2.5 AUTOLOGOUT 14

2.6 LOGGING 14

2.7 NETWORK AND IP OPTIONS 16

2.8 PROTOCOL ACCESS CONTROLS 17

3 SYSTEM ADMINISTRATION 18

3.1 STORAGE SYSTEM (HARDWARE) MANAGEMENT 19

3.2 DATA ONTAP (SOFTWARE) MANAGEMENT 22

3.3 ROLE-BASED ACCESS CONTROL (RBAC) 24

4 VULNERABILITY SCANNERS AND REPORTING 25

5 LICENSED PROTOCOLS 26

5.1 MULTISTORE 26

5.2 SNAPMIRROR 26

5.3 SNAPVAULT 27

5.4 CIFS 27

5.5 NFS 27

6 CONCLUSION 29

LIST OF TABLES

Table 1) Data ONTAP services and their default state. 7

Table 2) Options that control SSH connections after setup. 8

Table 3) Options that control SSL after setup (Data ONTAP 7.3.4). 10

Table 4) Options that control FilerView connections. 10

Table 5) Nonsecure services and their default states. 13

Table 6) Local storage system password attributes. 13

Table 7) Session timeouts and default settings. 14

Table 8) Data ONTAP log locations. 16

Table 9) IP options and recommended settings. 16

Table 10) Examples to block or unblock a protocol on an interface. 18
Table 11) Protocol filtering examples. 18
Table 12) BMC summary. 20
Table 13) SP summary. 20
Table 14) RLM summary. 21

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 virtual LANs (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 logical unit number (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 Network File System (NFS) and Common Internet File System (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 command line interface (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 might 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 Secure Shell (SSH) remote access as well as Secure Sockets Layer (SSL)–protected Web-based administration. NetApp strongly recommends these for use in all storage designs. Although Data ONTAP supports legacy clear-text protocols, 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 can be 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 can 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 Lightweight Directory Access Protocol (LDAP) over SSL for centralized authentication and authorization.
- Enable LDAP signing and sealing with Simple Authentication and Security Layer SASL.
- Enable CIFS signing to make sure of 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 access control lists (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 Storage Encryption self-encrypting drives, network-connected encryption appliances, or a combination of them to encrypt data at rest. If you do employ data encryption, a best practice is to make sure that your solution is fault tolerant by installing more than one encryption appliance and encryption key manager.

Make sure 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 to 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 create 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 dataset on a separate volume to make security configuration simpler.

2 INSTALLATION AND CONFIGURATION

There are several services that should be considered for disabling. Depending on your enterprise security structure, the state of any service depends on where the service is deployed and how deep it is in your infrastructure. The services contained in the following table do not require the purchase of additional licensing from NetApp. All of these settings are configurable through the `options` command.

Table 1) Data ONTAP services and their default state.

Service	Default State Data ONTAP 7.3.7
File Transfer Protocol (FTP)	Off
File Transfer Protocol over SSH (SFTP)	Off
File Transfer Protocol over SSL (FTPS)	Off
FilerView® https://<filer_IP>/na_admin (httpd.admin.ssl.enable)	Off
FilerView http://<filer_IP>/na_admin (httpd.admin.enable)	On
Network Data Management Protocol (NDMP)	Off
Remote Shell (rsh)	On
RIP – routed (RIPv1)	On
Secure Shell Service (ssh)	Off
Secure Shell v1 (SSHv1)	Off
Secure Shell v2 (SSHv2)	Off
Secure Sockets Service (ssl)	Off
Secure Sockets Layer v2 (SSLv2)	On
Secure Sockets Layer v3 (SSLv3)	On
Simple Network Management Protocol (SNMPv1) ("public" as a community string)	On
Simple Network Management Protocol (SNMPv3)	Off
Telnet	On
Transport Layer Security v1 (TLSv1)	Off
Trivial File Transfer Protocol (TFTP)	Off
WebDav	On

2.1 ENABLE SECURE ADMINISTRATIVE 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, the “Secure protocols and storage system access” section.

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 (CVE-2006-4924). SSH public keys provide a stronger and more granular method of SSH access to NetApp storage systems.

In Data ONTAP version 7.3.4 the option to disable sslv2 (options ssl.v2.enable off) was added. The modification of this option will provide the mitigation for CVE-2005-2969.

SETTING UP SSH

SSH is enabled by invoking the **`secureadmin setup ssh`** command at the CLI or through FilerView under SecureAdmin => SSH =>Configure. This will generate the keys and enable SSHv2.

```
cli> secureadmin setup ssh
SSH Setup
---------
Determining if SSH Setup has already been done before...no

SSH server supports both ssh1.x and ssh2.0 protocols.

SSH server needs two RSA keys to support ssh1.x protocol. The host key is
generated and saved to file /etc/sshd/ssh_host_key during setup. The server
key is re-generated every hour when SSH server is running.

SSH server needs a RSA host key and a DSA host key to support ssh2.0 protocol.
The host keys are generated and saved to /etc/sshd/ssh_host_rsa_key and
/etc/sshd/ssh_host_dsa_key files respectively during setup.

SSH Setup will now ask you for the sizes of the host and server keys.
 For ssh1.0 protocol, key sizes must be between 384 and 2048 bits.
 For ssh2.0 protocol, key sizes must be between 768 and 2048 bits.
 The size of the host and server keys must differ by at least 128 bits.

Please enter the size of host key for ssh1.x protocol [768] :
Please enter the size of server key for ssh1.x protocol [512] :
Please enter the size of host keys for ssh2.0 protocol [768] :

You have specified these parameters:
        host key size = 768 bits
        server key size = 512 bits
        host key size for ssh2.0 protocol = 768 bits
Is this correct? [yes]

Setup will now generate the host keys. It will take a minute.
After Setup is finished the SSH server will start automatically.

cli> Fri Jul 23 13:36:39 GMT [secureadmin.ssh.setup.success:info]: SSH setup is done
and ssh2 should be enabled. Host keys are stored in /etc/sshd/ssh_host_key,
/etc/sshd/ssh_host_rsa_key, and /etc/sshd/ssh_host_dsa_key.
```

Table 2) Options that control SSH connections after setup.

Option	Default	Recommended	Setting/CLI Command
ssh.access	*	Hosts or IP range	options ssh.access host=<hostname> options ssh.access host=aa.bb.cc.dd/mm Refer to the Manual Page Reference, Volume 2 - na_protocolaccess(8), for valid values
ssh.enable	On	On	options ssh.enable on

Option	Default	Recommended	Setting/CLI Command
ssh.passwd_auth.enable	On	On	options ssh.passwd_auth.enable on
ssh.idle.timeout	0	60	Controls orphaned connection - disconnect value in seconds options ssh.idle.timeout 60
ssh.port	22	22	options ssh.port 22
ssh.pubkey_auth.enable	On	On	options ssh.pubkey_auth.enable on
ssh1.enable	Off	Off	options ssh1.enable off
ssh2.enable	On	On	options ssh2.enable on
telnet.distinct.enable	Off	On	Enables making the ssh and console separate user environments; if set to OFF, ssh and the console will share the session options telnet.distinct.enable on
autologout.telnet.enable	On	On	Enables the automatic disconnect of inactive SSH Interactive sessions. options autologout.telnet.enable on
autologout.telnet.timeout	60	5	Timeout time in minutes. options autologout.telnet.timeout 5

SETTING UP SSL

The Secure Sockets Layer (SSL) protocol improves security by providing a digital certificate that authenticates storage systems and allows encrypted data to pass between the system and a browser. SSL is built into all major browsers. Therefore, installing a digital certificate on the storage system enables the SSL capabilities between system and browser.

Unlike using FilerView to send the storage system password in plain text, using SSL and Secure FilerView improves security by encrypting the administrator's password and all administrative communication when you manage your system from a browser.

Data ONTAP supports SSLv2 and SSLv3. You should use SSLv3 because it offers better security protections than previous SSL versions.

As a precautionary measure due to security vulnerability CVE-2009-3555, the SSL renegotiation feature is disabled in Data ONTAP. See Bug 386217: Data ONTAP impacted by OpenSSL Vulnerability CVE-2009-3555 for further details.

SSL is enabled by invoking the `secureadmin setup ssl` command at the CLI or through FilerView under SecureAdmin => SSL =>Configure.

Note: To enhance security, starting with Data ONTAP 7.3.5P1, Data ONTAP uses the SHA256 message-digest algorithm for generating a digital certificate.

The following is the output from the CLI:

```
cli> secureadmin setup ssl
Country Name (2 letter code) [US]:
State or Province Name (full name) [California]:
Locality Name (city, town, etc.) [Santa Clara]:
Organization Name (company) [Your Company]:
Organization Unit Name (division):
```

```
Common Name (fully qualified domain name) [company.com]:
Administrator email:
Days until expires [5475] :
Key length (bits) [512] :
Fri Jul 23 14:12:05 GMT [secureadmin.ssl.setup.success:info]: Starting SSL with new
certificate.
```

Table 3) Options that control SSL after setup (Data ONTAP 7.3.4).

Option	Default	Recommended	Setting/CLI Command
ssl.enable	On	On	options ssl.enable on
ssl.v2.enable	On	Off	options ssl.v2.enable off
ssl.v3.enable	On	On	options ssl.v3.enable on
tls.enable	Off	On	options tls.enable on

ENABLING SSL FOR FILERVIEW

By default FilerView is enabled on port 80, and this will pass all authentications in clear text. NetApp recommends that the ssl protocol be utilized for Web communication to the storage system for administrative functions. The following table contains the options to control the use of ssl for the session to FilerView.

Table 4) Options that control FilerView connections.

Option	Default	Recommended	Setting/CLI Command
httpd.admin.enable	On	Off	httpd.admin.enable off
httpd.admin.ssl.enable	Off	On	httpd.admin.ssl.enable on
httpd.timeout	300 seconds	300 seconds	Specifies the minimum amount of time (in seconds) before an idle HTTP connection will time out options httpd.timeout 300

2.2 DISABLE OR MODIFY DEFAULT ACCOUNTS

As stated in many of the Governance, Risk, and Compliance (GRC) Laws, Standards, and Doctrines, it is always considered and sometimes required to disable, delete, or modify the IT systems default authentication settings prior to placing the system in production.

Data ONTAP 7G has the following defaults, which should be modified prior to placing the storage system into production:

- root account
- naroot account (RLM, SP, BMC)
- snmp community string
- ndmp account and password encryption

ROOT ACCOUNT

The root account needs to be disabled in order to meet many, if not all, of the GRC standards. You will need to create a new administrative account prior to disabling root. Other functions that use this account such as NDMP and **ndmpcopy** might be affected. It will be necessary to use a different account for these functions. Details can be found in the Data Protection Tape Backup and Recovery Guide.

Best Practice: root
Create a new super administrator account and then disable "root." From the CLI: ontapSC> useradmin user add stgAdmin –g administrators ontapSC> options security.passwd.rootaccess.enable off From System Manager 2.0: Open the storage system, then, in the left pane, navigate to: Configuration =>local users and groups => users. With the user's pane in the right frame, click the "Create" icon. Once the new administrative account is created in System Manager, it will be necessary to use the CLI to disable the root account.

NAROOT ACCOUNT

The naroot account is the default account used to access the remote hardware management interfaces provided with the storage controllers. The password for the naroot account is the same as the password for the root account. For the RLM (firmware 4) and the SP the default account access can be disabled by disabling the root account.

Best Practice: naroot
RLM/SP Disable the Data ONTAP root account. BMC Disable the Data ONTAP root account and reset the password every 30 days.

SNMP

Data ONTAP 7G supports SNMP versions 1c, 2, and 3 (AuthNoPriv). There are many attacks that can be run against SNMP versions 1c/2 as they use a community string as the only control to access the queries for information. Data ONTAP 7G only supports read-only access. This can still provide a method for developing a footprint by an "uninvited guest." It is best to only utilize SNMPv3 to protect the access to the information that is provided by the OIDs. If you cannot use SNMPv3, at a minimum delete the default community string name and replace it with one that is not in the dictionary. The new community string should also contain special characters. This will reduce the likelihood of an attacker using a dictionary attack to guess the SNMPv1c/2 community string.

Best Practice: SNMPv3

Disable SNMPv1c/2 by removing the community string:

ontapSC> snmp community delete all

Create and SNMPv3 user:

Enter the following commands to create a role, group, and user with login-snmp capability:

ontapSC> useradmin role add snmpAuth -a login-snmp

ontapSC> useradmin group add snmpv3users -r snmpAuth

ontapSC> useradmin user add trapAdmin -g snmpv3users

Note: Refer to the "How to monitor your storage system with SNMP" section of the Data ONTAP 7.3.7 Storage Management Guide.

Best Practice: SNMPv1c/2

Modify the SNMP community string.

From the CLI:

```
ontapSC> snmp community delete all
ontapSC> snmp community add ro C0mmun!ty$tringNam3
```

From System Manager 2.0:

Open the storage system, then, in the left pane, navigate to:

Configuration => System Tools => SNMP.

In the right frame, select the Edit icon and modify the community name.

NDMP ACCOUNT AND PASSWORD ENCRYPTION

The NDMP function and the ndmpcopy function, by default, use the root account as well as pass the password using a challenge/response to the backup server or service.

Best Practice: ndmp/ndmpcopy

Create a service account for ndmp and ndmp copy use and assign this account to the "Backup Operators" group.

Use the ndmpd password command to generate a secure password:

```
ontapSC> useradmin user add ndmpsvc -g "Backup Operators"
New password:
Retype new password:
User <ndmpsvc> added.
ontapSC> ndmpd password ndmpsvc
```

2.3 DISABLE UNNECESSARY SERVICES

By default, telnet, RIPv1, rsh, and webdav are enabled. If these services are not required in your infrastructure, NetApp recommends that they be disabled. The following table contains the services that are on by default and the recommended settings.

Table 5) Nonsecure services and their default states.

Option	Default	Recommended	Setting/CLI Command
rsh.access	Legacy	Host or none	options rsh.access – Refer to the Manual Page Reference, Volume 2 - na_protocolaccess(8), for valid values
rsh.enable	On	Off	options rsh.enable off
telnet.access	Legacy	Host or none	options telnet.access – Refer to the Manual Page Reference, Volume 2 - na_protocolaccess(8), for valid values
telnet.distinct.enable	Off	On	options telnet.distinct.enable on This option also affects the SSH interactive sessions
telnet.enable	On	Off	options telnet.enable off
webdav.enable	On	Off	options webdav.enable off
routed	On	Off	RIPv1 port 520 not authenticated routed off

2.4 PASSWORD SECURITY

The following table contains the recommendations for the password properties. The “Data ONTAP Commands: Manual Page Reference, Volume 1” contains the security.passwd options to modify as well as the **`useradmin user`** command with the **`-m`** and **`-M`** options.

Table 6) Local storage system password attributes.

Rule	Default	Recommended	Setting/CLI Command
Root access	On	Off	options security.passwd.rootaccess.enable off
Apply to all accounts	Off	On	options security.passwd.rules.everyone on
Maximum age	4,294,967,295 days	90 days	useradmin user add <acct> -g <group> -M 90
Minimum age	0 days	1 day	useradmin user add <acct> -g <group> -m 1
Minimum length	8	8	options security.passwd.rules.minimum 8
Maximum length	None	14	options security.passwd.rules.maximum 14
Alpha characters	2	1	options security.passwd.rules.minimum.alphabetic 2

Rule	Default	Recommended	Setting/CLI Command
Numeric characters	1	1	options security.passwd.rules.minimum.digit 1
Special characters	0	1	options security.passwd.rules.minimum.symbol 1
History	6	6	options security.passwd.rules.history 6
Bad logon lockout	4,294,967,295	6	options security.passwd.lockout.numtries 6
Change on first logon	Off	On	options security.passwd.firstlogin.enable on

2.5 AUTOLOGOUT

The autologout capability is required by several security standards. In Data ONTAP these requirements can be met by setting the timeout times in the various interfaces. If the timeouts are enabled, the session will be terminated and will require reauthentication.

Warning: If you are connecting to an SSH using the NetApp remote LAN management (RLM) card, the service processor (SP), or the baseboard management controller (BMC), these options are ignored for the SSH interactive session. See the "Data ONTAP System Administration Guide" for further details.

Table 7 is a listing of the default and recommended settings for the options that control the timeout of the administrative sessions for Data ONTAP 7G and 7-Mode storage systems.

Table 7) Session timeouts and default settings.

Rule	Default	Recommended	Setting/CLI Command
Console timeout time	60	5	options autologout.console.timeout 5
Console timeout enable	On	On	options autologout.console.enable on
Telnet timeout time	60	5	options autologout.telnet.timeout 5
Telnet timeout enable	On	On	options autologout.telnet.enable on
SSH interactive timeout	60	5	options autologout.telnet.timeout 5
SSH interactive enable	On	On	options autologout.telnet.enable on
HTTP timeout	300	300	options httpd.timeout 300
SSH "orphan" timeout	0	300	options ssh.idle.timeout 300

2.6 LOGGING

Data ONTAP provides logging capabilities for many functions within the base operating system as well as many of the protocols; licensed services provide their own logging. The base logging of Data ONTAP includes an audit log and a messages log.

AUDIT LOG

An audit log is a record of commands executed at the console, through a telnet shell or an SSH shell, or by using the rsh command. All the commands executed in a source file script are also recorded in the audit log. Administrative HTTP operations, such as those resulting from the use of FilerView or other

Manage ONTAP® SDK-based applications, are logged. All log-in attempts to access the storage system, with success or failure, are also audit logged.

In addition, changes made to configuration and registry files are audited. Read-only APIs by default are not audited, but you can enable auditing with the auditlog.readonly_api.enable option. By default, Data ONTAP is configured to save an audit log. The audit log data is stored in the /etc/log directory in a file called auditlog.

For configuration changes, the audit log shows the following information:

- Which configuration files were accessed
- When the configuration files were accessed
- What has been changed in the configuration files

For commands executed through the console, a telnet shell, an SSH shell, or by using the rsh command, the audit log shows the following information:

- Which commands were executed
- Who executed the commands
- When the commands were executed

The maximum size of the audit-log file is specified by the auditlog.max_file_size option (default is about 10M). The maximum size of an audit entry in the audit-log file is 200 characters. An audit entry is truncated to 200 characters if it exceeds the size limit.

Every Saturday at midnight, the /etc/log/auditlog file is copied to /etc/log/auditlog.0, /etc/log/auditlog.0 is copied to /etc/log/auditlog.1, and so on. This also occurs if the audit-log file reaches the maximum size specified by auditlog.max_file_size.

The system saves audit-log files for six weeks, unless any audit-log file reaches the maximum size, in which case the oldest audit-log file is discarded.

You can access the audit-log files using your NFS or CIFS client, or using FilerView or NetApp System Manager.

Best Practice

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 might dictate central log collection and analysis. Data ONTAP does support the sending of Data ONTAP audit logs to an external syslog host. Although NetApp does not recommend using an external syslog as a best practice, consider this option as a way to collect historical data; see the syslog.conf file description and use in the man pages volume 2 for details.

MESSAGES LOG

This log is located in the /etc/log directory on the storage system and is written to by the syslogd daemon to print all logging messages of priority info or higher to the console and to the messages file. A typical message is:

```
Fri Jun 10 14:31:37 PDT 2005 [rc]: NetApp Release 7.3.4 boot complete.
```

Every Saturday at 24:00, /etc/messages is moved to /etc/messages.0, /etc/messages.0 is moved to /etc/messages.1, and so on. Message files are saved for a total of six weeks.

You can access the messages log files using your NFS or CIFS client, or using FilerView or NetApp System Manager.

Table 8) Data ONTAP log locations.

Log	Location
System audit log	/etc/log/auditlog
System messages log	/etc/log/messages
System EMS log	/etc/log/ems
CIFS audit log (active)	/etc/log/cifsaudit.alf
FTP command audit log	/etc/log/ftp.cmd
FTP transfer log	/etc/log/ftp.xfer
HTTP log	/etc/log/http.log
BMC SEL log	BMC Flash memory
RLM SEL log	RLM Flash memory
SP SEL log	SP Flash memory

2.7 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 (RIPv1) 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 Address Resolution Protocol (ARP) spoofing attacks. Enable packet checking to verify source IP addresses.

Table 9) IP options and recommended settings.

Option	Default	Recommended	Setting/CLI Command
ip.fastpath.enable	On	Off	options ip.fastpath.enable off
ip.icmp_ignore_redirect.enable	Off	On	options ip.icmp_ignore_redirect.enable on
ip.match_any_ifaddr	On	Off	options ip.match_any_ifaddr off
ip.ping_throttle.alarm_interval	0	15	options ip.ping_throttle.alarm_interval 15

Option	Default	Recommended	Setting/CLI Command
ip.ping_throttle.drop_level	150	100	options ip.ping_throttle.drop_level 100
routed	On	Off	routed off

IP.FASTPATH.ENABLE

The NetApp storage system attempts to use MAC address and interface caching (fastpath) 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.

This can lead to higher availability of ARP spoofing and session hijacking attacks.

IP.ICMP_IGNORE_REDIRECT.ENABLE

You can disable Internet Control Message Protocol (ICMP) redirect messages to protect your storage system against forged ICMP redirect attacks.

To efficiently route a series of datagrams to the same destination, your storage system maintains a route cache of mappings to next-hop gateways. If a gateway is not the best next hop for a datagram with a specific destination, the gateway forwards the datagram to the best next-hop gateway and sends an ICMP redirect message to the storage system. By forging ICMP redirect messages, an attacker can modify the route cache on your storage system, causing it to send all of its communications through the attacker. The attacker can then hijack a session at the network level, easily monitoring, modifying, and injecting data into the session.

IP.MATCH_ANY_IFADDR

If the option is on, the storage system will accept any packet that is addressed to it even if that packet came in on the wrong interface.

IP.PING_THROTTLE.ALARM_INTERVAL

Specifies in minutes how often dropped pings will be syslogged. This prevents a ping flood denial of service attack from flooding the syslog with messages. A value of 0 turns off logging of ping floods.

IP.PING_THROTTLE.DROP_LEVEL

Specifies the maximum number of ICMP echo or echo reply packets (ping packets) that the storage system will accept per second. All further packets within one second are dropped to prevent ping flood denial of service attacks.

2.8 PROTOCOL ACCESS CONTROLS

Data ONTAP has two ways to control protocol access to a FAS storage system. They are protocol blocking and protocol access filtering. NetApp recommends that you use both of these options in all environments in which 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.

Table 10) Examples to block or unblock a protocol on an interface.

Block Protocol	Interface	Setting/CLI Command d
CIFS	e0c	options interface.blocked.cifs e0c
ftpd	e0f	options interface.blocked.ftpd e0f
iSCSI	e2b	options interface.blocked.iscsi e2b
NFS	allow/reset	options interface.blocked.nfs “”
SnapMirror®	e4a, e1b	options interface.blocked.snapmirror e4a,e1b
User Data	e0M	options interface.blocked.mgmt_data_traffic on
ndmp	e1a	options interface.blocked.ndmp e1a

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 host names, 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 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.

Table 11) Protocol filtering examples.

Protocol	Filter Type	Setting/CLI Command
rsh	Host	options rsh.access host=lima
telnet	IP subnet	options telnet.access host=192.168.19.0/24
ssh	Host and interface e0g	options ssh.access “host=mng,uws AND if=e0g”
snmp	Host	options snmp.access host=wks219ht
httpd	Block all access	options httpd.access host=-

3 SYSTEM ADMINISTRATION

Data ONTAP enables you to control access to your storage system to provide increased security and auditing capability. It also enables you to manage passwords on the storage system to provide security.

You can use the default system administration account, or root, for managing a storage system. However, NetApp highly recommends that you create additional administrator user accounts for the management of the storage system and disable the root account. This is a requirement of several security standards that call for all default accounts to be disabled. The root account in Data ONTAP 7.3.x does not require a password on setup. NetApp highly recommends that a password be assigned to the root account.

The following are the reasons for creating administrator accounts:

- You can specify that administrators and groups of administrators have differing degrees of administrative access to your storage systems.
- You can limit an administrator's access to specific storage systems by giving them an administrative account on only those systems.
- Having different administrative users allows you to display information about who is performing which commands on the storage system.
- The audit-log file keeps a record of all administrator operations performed on the storage system and the administrator who performed it, as well as any operations that failed due to insufficient capabilities.
- You assign each administrator to one or more groups whose assigned roles (sets of capabilities) determine what operations that administrator is authorized to carry out on the storage system.
- If a storage system running CIFS is a member of a domain or a Windows® work group, domain user accounts authenticated on the Windows domain can access the storage system using telnet, RSH, SSH, FilerView, Data ONTAP APIs, and Windows remote procedure calls (RPCs).

There are several management capabilities provided by the NetApp hardware and Data ONTAP.

You can manage your storage system remotely by using a remote management device:

- Service processor (SP)
- Remote LAN module (RLM)
- Baseboard management controller (BMC)

The remote management device stays operational regardless of the operating state of the storage system. It provides remote platform management capabilities, including remote access, monitoring, troubleshooting, logging, and alerting features.

To manage Data ONTAP and the configuration of the storage, the options that are available are:

- System console port
- e0M port (where available)
- Any configured Ethernet port

3.1 STORAGE SYSTEM (HARDWARE) MANAGEMENT

BASEBOARD MANAGEMENT CONTROLLER (BMC)

The baseboard management controller (BMC) is a remote management device that is built into the motherboard of FAS20xx storage systems. It provides remote platform management capabilities, including remote access, monitoring, troubleshooting, logging, and alerting features.

The BMC supports the SSH protocol for CLI access from UNIX® clients and PuTTY for CLI access from PC clients. Telnet and RSH are not supported on the BMC, and system options to enable or disable them have no effect on the BMC.

You can use "`root`," "`naroot`," or "`Administrator`" to log into the BMC. These users have access to all commands available on the BMC. *The password for all three account names is the same as the Data ONTAP* `root` *password.* You cannot add additional users to the BMC.

For detailed information on the BMC and its capabilities, refer to the "Using the Baseboard Management Controller for remote system management" section of the "Data ONTAP 7.3.7 System Administration Guide."

Note: The BMC uses the Data ONTAP `root` password (even if the `root` account is disabled) to allow access over the LAN with SSH. To access the BMC using SSH, you must configure the Data ONTAP `root` password. BMC accepts passwords that are no more than 16 characters.

Table 12) BMC summary.

Storage Systems	Connection Protocol	Current Firmware	Idle Connection Timeout	Failed Login IP Lockout
FAS20xx	SSHv2	1.3	None	No

Best Practice

Place the interface on a management VLAN or separate network from the user data access path.

Set a strong password for the Data ONTAP `root` account.

Change the `root` account password after each use.

Determine that the `root` account is disabled after you reset the password. When you reset the password on `root`, the `root` account becomes active. To disable the root account:

```
options security.passwd.rootaccess.enable off
```

Note: Make sure you have created another administrative account before disabling the root account.

SERVICE PROCESSOR (SP)

The SP CLI commands enable you to remotely access and administer the storage system and diagnose error conditions. Also, the SP extends AutoSupport™ capabilities by sending alerts and notifications through an AutoSupport message.

In order to access the storage system through the SP interface, an account must have `login-sp` capability. The storage system administrators group has `login-sp` capability by default. If the `root` local account is disabled, then the `naroot` account is disabled, and a local user with `login-sp` capability can log in to the SP.

SP firmware 1.2 and later will track failed SSH login attempts from an IP address. If more than 5 repeated login failures are detected from an IP address in any 10-minute period, the SP will stop all communication with that IP address for the next 15 minutes. Normal communication will resume after 15 minutes, but if repeated login failures are detected again, communication will again be suspended for the next 15 minutes.

For detailed information on the SP and its capabilities, refer to the “Using the service processor for remote system management” section of the “Data ONTAP 7.3.7 System Administration Guide.”

Table 13) SP summary.

Storage Systems	Connection Protocol	Current Firmware	Idle Connection Timeout	Failed Login IP Lockout
FAS32xx	SSHv2	1.2.2	None	Yes

Best Practice

Place the interface on a management VLAN or separate network from the user data access path.

Disable the `root` account and utilize accounts that are members of the storage system's administrators group to manage the storage system through the SP.

REMOTE LAN MODULE (RLM)

The RLM CLI commands enable you to remotely access and administer the storage system and diagnose error conditions. Also, the RLM extends AutoSupport capabilities by sending alerts and notifications through an AutoSupport message.

In order to access the storage system through the RLM interface, an account must have `login-sp` capability. The storage system administrators group has `login-sp` capability by default. If the `root` local account is disabled, then the `naroot` account is disabled, and a local user with `login-sp` capability can log in to the RLM.

RLM firmware 4.0 and above utilizes SSHv2 only. The SSH protocol on the RLM is part of the RLM's kernel operating system and therefore segmented from the implementation of SSH by the Data ONTAP operating system.

RLM firmware 4.0 will track failed SSH login attempts from an IP address. If more than 5 repeated login failures are detected from an IP address in any 10-minute period, the RLM will stop all communication with that IP address for the next 15 minutes. Normal communication will resume after 15 minutes, but if repeated login failures are detected again, communication will again be suspended for the next 15 minutes.

For detailed information on the RLM and its capabilities, refer to the "Using the Remote LAN Module for remote system management" section of the "Data ONTAP 7.3.7 System Administration Guide."

Table 14) RLM summary.

Storage Systems	Connection Protocol	Current Firmware	Idle Connection Timeout	Failed Login IP Lockout
FAS30xx	SSHv2	4.0	None	Yes
FAS31xx	SSHv2	4.0	None	Yes
FAS60xx	SSHv2	4.0	None	Yes

Best Practice

Place the interface on a management VLAN or separate network from the user data access path.

Disable the `root` account and utilize accounts that are members of the storage system's administrators group to manage the storage system through the RLM.

Determine that the FW is version 4.0 or later.

3.2 DATA ONTAP (SOFTWARE) MANAGEMENT

To access the storage system, you only need network connectivity to the storage system and authentication privileges; no licenses are required.

From the Ethernet network interface card (NIC) that is preinstalled in the storage system, connect to a TCP/IP network to administer the storage system:

- From any client using FilerView
- From any client by using System Manager
- From any client by using a telnet session
- From any client by using a Remote Shell connection
- From any client by using a Secure Shell connection
- From the hardware management device (RLM/SP/BMC)

SYSTEM MANAGER

System Manager (a primary GUI management tool) provides access using port 80/443. It is available on all platforms.

System Manager is a graphical management interface that enables you to manage most storage system functions through a telnet session, the rsh command, or scripts or configuration files rather than by entering commands at the console. You can also use System Manager to view information about the storage system; its physical storage units, such as adapters, disks, and RAID groups; and its data storage units, such as aggregates, volumes, and LUNs.

Best Practice

Configure and use the e0M port as the Data ONTAP management port.

Place the interface (e0M) on a management VLAN or separate network than the user data access path.

Set/verify the following options:

- httpd.admin.ssl.enable (Off by default): Enables HTTPS (port 443) access for System Manager.
  ```
  options httpd.admin.ssl.enable on
  ```
- tls.enable: Enables tls, more secure than sslv3 and required in some environments (Off by default).
  ```
  options tls.enable on
  ```

The following are other options that affect access for System Manager:

- httpd.admin.access (On by default): Restricts HTTP access to System Manager. If this value is set, trusted.hosts is ignored for System Manager access.

Note: Can be used in situations where the host listed is in a physically controlled space and only highly trusted personnel have access to the host.

- httpd.admin.enable (On by default): Enables HTTP (port 80) access to System Manager.
- http.admin.hostsequiv.enable (Off by default): Enables the use of /etc/hosts.equiv for administrative HTTP authentication. If enabled, the authentication of administrative HTTP (for APIs) will use the contents of /etc/hosts.equiv to allow access to the storage controller without the need to provide a password.

Note: Use care when adding hosts to the /etc/host.equiv file on the storage system. If http.admin.hostsequiv.enable is set to On, administrative access is granted based on the username that is part of the /etc/host.equiv file. NO PASSWORD IS REQUIRED.

TELNET

Clear text passwords are passed between the client and the storage system.

The telnet.distinct.enable option enables making the telnet and console separate user environments. If it is off, then telnet and the console share a session. The two sessions view each other's inputs/outputs, and both acquire the privileges of the last user to log in. If this option is toggled during a telnet session, then it goes into effect on the next telnet login. Valid values for this option are On and Off. This option is set to On if a user belonging to "compliance administrators" is configured and cannot be set to Off until the user is deleted. The default setting is Off.

You configure a banner message to appear at the beginning of a telnet session to a storage system by creating a file called /etc/issue. The message only appears at the beginning of the session. It is not repeated if there are multiple failures when attempting to log in.

Note: The /etc/issue file can be created from the storage system CLI using the `wrfile` command. For more information on how this is accomplished, refer to the "Writing a WAFL file" section of the "Data ONTAP 7.3.7 System Administration Guide."

There are two option settings that control the auto logout of the telnet session: autologout.telnet.enable and autologout.telnet.timeout. Auto logout for the telnet session is enabled by default with a timeout setting of 60 minutes.

Best Practice: Telnet

If telnet is used, set the following options:

- Distinct sessions from the console session:
  ```
  options telnet.distinct.enable on
  ```
- Session timeout to a value of 5 minutes:
  ```
  options autologout.telnet.enable on
  options autologout.telnet.timeout 5
  ```
- Set a banner message through the creation of the /etc/issue file.

For detailed information on telnet and its capabilities, refer to the "Telnet sessions and storage system access" section of the "Data ONTAP 7.3.7 System Administration Guide."

RSH

Clear text passwords are passed between the client and the storage system.

Best Practice: RSH

Take care when using this protocol to maintain the storage and take precautions so that your passwords and user IDs are not compromised in transit from the client to the storage system.

To disable RSH: `options rsh.enable off`

For detailed information on RSH and its capabilities, refer to the "How to access a storage system using a Remote Shell connection" section of the "Data ONTAP 7.3.7 System Administration Guide."

SSH

The `secureadmin setup ssh` command configures the SSH server. The administrator specifies the key strength for the RSA host and server keys. The keys can range in strength from 384 to 2,048 bits.

If your storage system does not have SSH enabled, you can set up SecureAdmin to enable secure sessions using SSH. A few options enable you to control password-based authentication and public key authentication, control access to a storage system, and assign the port number to a storage system.

SecureAdmin is set up automatically on storage systems shipped with Data ONTAP 8.0 or later.

A post-log-in banner is available for the sshv2 protocol. The banner that is used is read from the /etc/motd file. To activate this banner, set the option ssh2.banner.enable to On. This option does not exist until it is created.

Note: The /etc/motd file can be created from the storage system CLI using the `wrfile` command. For more information on how this is accomplished, refer to the "Writing a WAFL file" section of the "Data ONTAP 7.3.7 System Administration Guide."

Best Practice: SSH
• Determine that ssh1 is disabled; only ssh2 is enabled. **options ssh (will display all the ssh settings)** **options ssh1.enable off (disables sshv1)** **options ssh2.enable on (enables sshv2)** • Set active session timeout for 5 minutes; SSH session timeout is controlled by the telnet timeout settings. **options autologout.telnet.enable on** **options autologout.telnet.timeout 5** • Set distinct sessions from the console session. **options telnet.distinct.enable on** • Set orphaned SSH session timeout to 1 minute (60 seconds). **options ssh.idle.timeout 60** • Create a banner for the ssh session by creating a /etc/motd file. • Enable the sshv2 banner. **options ssh2.banner.enable on**

For detailed information on SSH and its capabilities, refer to the "SSH protocol" section of the "Data ONTAP 7.3.7 System Administration Guide."

For detailed information on the `secureadmin` command, refer to the "secureadmin" section of the "Data ONTAP 7.3.7 Commands: Manual Page Reference," Volume 1.

HARDWARE MANAGEMENT RLM/SP/BMC

Once you have a established a session with the RLM/SP/BMC, you can access the Data ONTAP CLI by issuing the **`system console`** command.

3.3 ROLE-BASED ACCESS CONTROL (RBAC)

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 that you can modify. You can also create new roles. Again, when you create 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 7.3.4 uses six types of capabilities:

- **API rights.** These capabilities have names that begin with “api-" and are used to control which application programming interface (API) commands you can use. API commands are usually executed by programs, rather than directly by administrators.
- **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 CLI.
- **Compliance rights.** These capabilities provide the ability to execute compliance-related operations.
- **FilerView read-only right.** This right grants read-only access to FilerView. “filerview-readonly” is not assigned to a role by default.
- **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.
- **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 VULNERABILITY SCANNERS AND REPORTING

In order to understand the results of security scanners, it is important to understand some aspects of how they operate. Very rarely do the scanners perform actual tests of devices for security vulnerabilities. Some security scanners operate by making assumptions about the capabilities of the devices they are scanning based on release version identifiers found in the scanned devices. If the release version identifiers contained in the scanned devices, and more particularly in the software running on those devices, identifies a release that contains a suspected vulnerability even though that issue has subsequently being remediated, the security scanner can report “false-positive” indications of the presence of security vulnerabilities when they do not actually exist.

For instance, Data ONTAP and other NetApp products are heavily modified over time as new features are introduced and as suspected security vulnerabilities are identified and remediated. Applicable licenses of components of NetApp products often require the original, rather than the current, effective release version identifier be used in the code. As a result, based on those revision strings, the scanners might report that NetApp products are not completely up to date and therefore suspected security vulnerabilities have not been remediated, when, in fact, they have.

When customers seek advice about those suspected issues, it assists us enormously to have the customer provide the relevant CVE or VU number reported by the scanner. NetApp tracks any such issues with their associated CVE and VU numbers. To assist the NetApp field and its customers, we are

working on getting relevant CVE or VU numbers visible through “Bugs” online on the NetApp Support (formerly NOW®) site so that they can search directly on those identifiers.

CVE or VU numbers are unique, industry-wide identifiers for publicly known data security vulnerabilities and exposures. Common, publicly available cross-reference tables of possible interest for NetApp products are CERT, CERT-VN, Microsoft®, and BUGTRAQ (Apache, in DFM/OM products). The map of cross-references is too dynamic to reproduce on our support site. We rely on the Computer Emergency Response Team (CERT) and Mitre to keep the various cross-reference tables up to date; mitre.org has a comprehensive set of cross-reference tables between CVE numbers and other tracking systems at http://cve.mitre.org/data/refs/index.html.

NetApp policy is to respond to reports of actual vulnerabilities that include enough diagnostic data for us to act on. Vulnerability reports should be made to the Global Support organization as regular bugs, except that you should ask for the case to be escalated to the Vulnerability Response team.

Refer to the Suspected Security Vulnerabilities page on the NetApp Support site: http://now.netapp.com/NOW/knowledge/docs/olio/scanner_results/.

5 LICENSED PROTOCOLS

Each of the licensed protocols has its own specific recommendations for administration.

5.1 MULTISTORE

MultiStore enables you to partition the storage and network resources of a single storage system so that it appears as multiple storage systems on the network. MultiStore is optional software that is available by license for Data ONTAP.

Each storage system created as a result of the partitioning is called a vFiler® unit. A vFiler unit, using the resources assigned, delivers file services to its clients as a storage system does.

The storage resource assigned to a vFiler unit can be one or more qtrees or volumes. The network resource assigned can be one or more base IP addresses or IP aliases associated with network interfaces.

Settings to manage and audit the MultiStore protocol can be found in the following references:

“Data ONTAP 7.3.7 MultiStore Management Guide”

“NetApp MultiStore: An Independent Security Analysis” by Matasano Security

5.2 SNAPMIRROR

SnapMirror is a feature of Data ONTAP that enables you to replicate data. SnapMirror enables you to replicate data from specified source volumes or qtrees to specified destination volumes or qtrees, respectively. You need a separate license to use SnapMirror.

Settings to manage and audit the SnapMirror protocol can be found in the following references:

“Data ONTAP 7.3.7 Data Protection Online Backup and Recovery Guide” in the “Data protection using SnapMirror” section

“SnapMirror Async Overview and Best Practices Guide” (TR-3446)

5.3 SNAPVAULT

SnapVault leverages disk-based backup and block-level incremental backups for reliable, low-overhead backup and recovery suitable for any environment. SnapVault enables data stored on multiple systems to be backed up to a central secondary system quickly and efficiently as read-only Snapshot™ copies.

Settings to manage and audit the SnapVault protocol can be found in the following references:

“Data ONTAP 7.3.7 Data Protection Online Backup and Recovery Guide” in the “Data protection using SnapVault” section

“SnapVault Best Practices Guide” (TR-3487)

5.4 CIFS

Data ONTAP 7.3.x provides support (license required) for the CIFS protocol, which is documented in an Internet Engineering Task Force (IETF) draft specification titled "A Common Internet File System (CIFS/1.0) Protocol."

CIFS is a file-sharing protocol intended to provide an open cross-platform mechanism for client systems to request file services from server systems over a network. It is based on the standard Server Message Block (SMB) protocol widely in use by personal computers and workstations running a wide variety of operating systems.

Settings to manage and audit the CIFS protocol can be found in the following references:

“Data ONTAP 7.3.7 File Access and Protocols Management Guide” in the “File access using CIFS” and “File sharing between NFS and CIFS” sections

“NetApp Storage Systems in a Microsoft Windows Environment” (TR-3367)

“Windows File Services Best Practices with NetApp Storage Systems” (TR-3771)

“Auditing Quick Start Guide” (TR-3595)

“Bulk Security Quick Start Guide” (TR-3597)

“SMB 2.0—Next-Generation CIFS Protocol in Data ONTAP” (TR-3740)

“FPolicy Safeguards in Data ONTAP” (TR-3640)

5.5 NFS

Data ONTAP 7.3.x supports versions 2, 3, and 4 of the NFS protocol, which are documented in RFCs 1094, 1813, and 3530, respectively.

NFS is a widely used file-sharing protocol supported on a broad range of platforms. The protocol is designed to be stateless, allowing easy recovery in the event of server failure. Associated with the NFS protocol are two ancillary protocols, the MOUNT protocol and the NLM protocol. The MOUNT protocol provides a means of translating an initial path name on a server to an NFS file handle that provides the initial reference for subsequent NFS protocol operations. The NLM protocol provides file-locking services, which are stateful by nature, outside of the stateless NFS protocol. NFS is supported on both TCP and UDP transports.

Support for TCP and UDP is enabled by default. Either one can be disabled by setting the nfs.tcp.enable or nfs.udp.enable options using the `options` command.

Settings to manage and audit the NFS protocol can be found in the following references:

“Data ONTAP 7.3.7 File Access and Protocols Management Guide” in the “File access using NFS” and “File sharing between NFS and CIFS” sections

“NFS v4 Enhancements and Best Practices Guide—Data ONTAP Implementation” (TR-3580)

“NetApp Storage System Multiprotocol User Guide” (TR-3490)

“NFS v3 Enhancements in Data ONTAP 7.2.1” (TR-3550)

“Export and Network Changes Between Data ONTAP 7.0.5 and 7.2.4” (TR-3706)

6 CONCLUSION

Data ONTAP is and always has been an operating system. Within Data ONTAP there are two distinct types of access: user data access through the NAS and SAN modules, and administrative access through the storage controllers' administrative module. Care needs to be taken when assigning elevated administrative access.

Data ONTAP has many security-related options that can be set to meet your particular needs. NetApp strongly recommends that you use secure administration methods for Data ONTAP and that you disable any administrative protocols you deem to be a high risk for your environment.

NetApp
www.netapp.com