Technical Report

# PCI-DSS Version 2.0 and Data ONTAP 8.1

Ron Demery, NetApp

November 2011 | TR-3996

## GUIDANCE FOR USING DATA ONTAP OPERATING IN 7-MODE

This TR is targeted at qualified security assessors as well as storage administrators. Guidance is provided for the requirements that have controls that can be applied within the Data ONTAP® operating system. Although this document focuses on Data ONTAP version 8.1 operating in 7-Mode, many of these settings may apply to earlier versions of Data ONTAP 7G and Data ONTAP operating in 7-Mode.

## TABLE OF CONTENTS

## LIST OF TABLES

# 1 INTRODUCTION TO PCI-DSS

This technical report provides guidance and information that auditors and system operators will find useful in applying the Payment Card Industry (PCI) Data Security Standard (DSS) requirements to a storage system that is running the Data ONTAP operating system.

Data ONTAP offers two modes of access, one for administration and one for user data. This paper focuses on the administration of the system configuration, because many of the user data requirements are met by the applications that have governance over the data and not the storage systems.

In a review of the PCI-DSS standard, some controls must be considered in the Data ONTAP 7G and 7-Mode operating systems for PCI-DSS requirements 1, 2, 5, 6, 8, 9, and 10. If the NetApp® storage system has the optional MultiStore® software license, then Appendix A, "Additional PCI-DSS Requirements for Shared Hosting Providers," also applies.

# 2 BUILD AND MAINTAIN A SECURE NETWORK

## REQUIREMENT 1: INSTALL AND MAINTAIN A FIREWALL CONFIGURATION TO PROTECT CARDHOLDER DATA

Requirement 1 of the PCI-DSS version 2 standard states:

> Firewalls are devices that control computer traffic allowed between an entity's networks (internal) and untrusted networks (external), as well as traffic into and out of more sensitive areas within an entity's internal trusted networks. The cardholder data environment is an example of a more sensitive area within an entity's trusted network.
>
> A firewall examines all network traffic and blocks those transmissions that do not meet the specified security criteria.
>
> All systems must be protected from unauthorized access from untrusted networks, whether entering the system via the Internet as e-commerce, employee Internet access through desktop browsers, employee e-mail access, dedicated connections such as business-to-business connections, via wireless networks, or via other sources. Often, seemingly insignificant paths to and from untrusted networks can provide unprotected pathways into key systems. Firewalls are a key protection mechanism for any computer network.
>
> Other system components may provide firewall functionality, provided they meet the minimum requirements for firewalls as provided in Requirement 1. Where other system components are used within the cardholder data environment to provide firewall functionality, these devices must be included within the scope and assessment of Requirement 1.

If the storage system is used in a NAS or iSAN configuration, protocol filters placed on the network interface can be configured to limit the type of connections to the (CIFS, NFS, SnapMirror®, iSCSI, etc.) network port.

### 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 1) Protocol blocking examples.

| Block Protocol | Interface | Setting / CLI Command |
|---|---|---|
| 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 |

### PROTOCOL ACCESS FILTER

Data ONTAP allows the configuration of filters for the following protocols: RSH, telnet, SSH, HTTP, SNMP, NDMP, SnapMirror, and SnapVault® software. 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 2) Protocol access filter 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=- |

## REQUIREMENT 2: DO NOT USE VENDOR-SUPPLIED DEFAULTS FOR SYSTEM PASSWORDS AND OTHER SECURITY PARAMETERS

Requirement 2 of the PCI-DSS version 2 standard states:

*Malicious individuals (external and internal to an entity) often use vendor default passwords and other vendor default settings to compromise systems. These passwords and settings are well known by hacker communities and are easily determined via public information.*

The default accounts that are part of Data ONTAP 7G and 7-Mode are:

- root
- diag (Data ONTAP 8.0 and greater)

- naroot (BMC, RLM, SP)
- SNMP community string

For detailed information on user account management, please refer to the “How to manage administrator and diagnostic access” section of the “Data ONTAP 8.1 7-Mode System Administration Guide.”

## SECTION 2.1 VENDOR-SUPPLIED DEFAULTS

Always change vendor-supplied defaults, including but not limited to passwords, simple network management protocol (SNMP) community strings, and elimination of unnecessary accounts, before installing a system on the network.

### Best Practice - root account

Create a new super administrator account and then disable ‘root.’
From the CLI:

```
ontapSC> useradmin user add newadmin –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 in the "Create" icon.

Once the new administrative account is created it will be necessary to use the CLI to disable the root account.

### Best Practice - diag user

Determine that the ‘diag’ user account is disabled after each use.
Only available from the CLI:
Keep the diag account disabled when not in use.

```
ontapSC> priv set advanced

ontapSC*> useradmin diaguser lock

ontapSC*> useradmin diaguser show
```

Reset the password on every use.

```
ontapSC> priv set advanced

ontapSC*> useradmin diaguser password
```

### Best Practice - RLM/SP/BMC

Any account that is a member of the Data ONTAP ‘administrators’ group has permission to log on to these interfaces.
The RLM will disable the ‘naroot’ account if the Data ONTAP ‘root’ account is disabled.
The SP and the BMC will continue to use the password of the Data ONTAP ‘root’ account for the ‘naroot’ account.

**Best Practice – SNMP**

Modify the SNMP community string.
From the CLI:

```
ontapSC> snmp community delete all
ontapSC> snmp community add ro CommunityStringName
```

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.

### SECTION 2.2.2 ENABLE ONLY NECESSARY AND SECURE SERVICES, PROTOCOLS, DAEMONS, ETC., AS REQUIRED FOR THE FUNCTION OF THE SYSTEM

**Table 3) Services and defaults for a clean installation of Data ONTAP 8.1 operating in 7-Mode.**

| Service | Default State | Recommended | Command |
|---|---|---|---|
| ndmp | off | off (if not needed) | `ndmpd off` |
| Telnet | off | off | `options telnet.enable off` |
| SSLv2 | off | off | `options sslv2.enable off` |
| SSLv3 | on | on | `options ssl.v3.enable on` |
| TLSv1 | off | on | `options tls.enable on` |
| SSH | on | on | `options ssh.enable on` |
| SSHv1 | off | off | `options ssh1.enable off` |
| SSHv2 | on | on | `options ssh2.enable on` |
| RSH | off | off | `options rsh.enable off` |
| RIP | off | off | `routed off` |
| WebDav | on | off | `options webdav.enable off` |
| FTP | off | off | `options fptd.enable off` |

### SECTION 2.3 ENCRYPT ALL NONCONSOLE ADMINISTRATIVE ACCESS USING STRONG CRYPTOGRAPHY

**Recommendation**

Use sshv2 or TLS for administrative sessions with the storage system.

# 3 PROTECT CARDHOLDER DATA

### REQUIREMENT 3: PROTECT STORED CARDHOLDER DATA

With the release of Data ONTAP 8.1, NetApp storage encryption (NSE) introduces the ability to encrypt cardholder data at rest through encrypting hard drives. When paired with a supported key management solution, this should help satisfy requirements in sections 3.4, 3.5, and 3.6. There are several external solutions for data-at-rest encryption that are available through NetApp. These solutions can be further investigated by visiting http://www.netapp.com/us/solutions/infrastructure/storage-security.

### REQUIREMENT 4: ENCRYPT TRANSMISSION OF CARDHOLDER DATA ACROSS OPEN PUBLIC NETWORKS

Recommend the use of VPN tunnels or other bulk encryption methods for the movement of data.

# 4 MAINTAIN A VULNERABILITY MANAGEMENT PROGRAM

### REQUIREMENT 5: USE AND REGULARLY UPDATE ANTIVIRUS SOFTWARE OR PROGRAMS

Requirement 5 of the PCI-DSS version 2 standard states:

> Malicious software, commonly referred to as “malware”—including viruses, worms, and Trojans—enters the network during many business approved activities including employee e-mail and use of the Internet, mobile computers, and storage devices, resulting in the exploitation of system vulnerabilities. Anti-virus software must be used on all systems commonly affected by malware to protect systems from current and evolving malicious software threats.

If the storage controller is in a SAN configuration the AV scanner will access the user data files via the host operating system. If it is in a NAS configuration the AV scanner can only integrate the CIFS shares.

NetApp integrated antivirus software (from Computer Associates, McAfee, Sophos, Symantec, and Trend Micro) provides additional protection against viruses by scanning files accessed by Windows® and CIFS/SMB clients. The virus-scanning activity is transparent to end users and occurs before the file is committed to disk (write requests) or delivered to the requesting user or application (read requests).

From Data ONTAP 7.2 onward write scanning functionality has changed. The file is committed to disk before scanning completes: that is, there is no waiting time, and it improves the end-user experience. In case a virus is found after the write operation, the file will be marked as infected and will not be accessible.

For more information, refer to http://www.netapp.com/us/products/storage-security-systems/antivirus/ or the “Data Protection, Online Backup, and Recovery Guide” for your version of Data ONTAP and the “Antivirus Scanning Best Practices Guide” (TR-3107).

### REQUIREMENT 6: DEVELOP AND MAINTAIN SECURE SYSTEMS AND APPLICATIONS

Requirement 6 of the PCI-DSS version 2 standard states:

> Unscrupulous individuals use security vulnerabilities to gain privileged access to systems. Many of these vulnerabilities are fixed by vendor provided security patches, which must be installed by the entities that manage the systems. All critical systems must have the most recently released, appropriate software patches to protect against exploitation and compromise of cardholder data by malicious individuals and malicious software.

| Recommendation |
|---|
| Stay as current as possible with the GA-designated releases of Data ONTAP. |

### VULNERABILITY SCANS OF DATA ONTAP 7G AND 7-MODE SYSTEMS

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 identify a release that contains a suspected vulnerability even though that issue has subsequently been 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 for components of NetApp products often require that 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 may report that NetApp products are not completely up to date and that therefore suspected security vulnerabilities have not been remediated when, if fact, they have.

The versions of OpenSSH (and OpenSSL) code incorporated into Data ONTAP are declared by using the version string from which they were originally derived according to the licensing agreements. However, the code has been heavily customized for use in Data ONTAP, and our assessments show that the functions that needed to be vulnerable to the suspected issues raised do not exist in Data ONTAP.

The following shows the results that are commonly seen with some vulnerability scanners and the associated responses.

Table 4) Common SSL/SSH scanner results.

| CVE | Title | Description | Determination |
|---|---|---|---|
| CVE-2003-0386 | ReverseMapping | CVE-2003-0386<br>OpenSSH 3.6.1 and earlier, when restricting host access by numeric IP addresses and with VerifyReverseMapping disabled, allow remote attackers to bypass "from=" and "user@host" address restrictions by connecting to a host from a system whose reverse DNS host name contains the numeric IP address. | NOW Site Bug: 415008<br>False positive. Data ONTAP 7G and 7-Mode systems' implementation of SSH does not support host-based access control and therefore is not vulnerable. |
| CVE-2003-0682 | OpenSSH3.7.1 Memory Bugs | CVE-2003-0682<br>"Memory bugs" in OpenSSH 3.7.1 and earlier, with unknown impact, have a different set of vulnerabilities than CVE-2003-0693 and CVE-2003-0695. Provides unauthorized access. Allows partial confidentiality, integrity, and availability violation. Allows unauthorized disclosure of information. Allows disruption of service. | NOW Site Bug: 104381<br>False positive in 7.3.x. |

| CVE | Title | Description | Determination |
|---|---|---|---|
| CVE-2003-0693 | OpenSSH 3.7.0 Buffer Overflow | CVE-2003-0693<br>US-CERT Vulnerability Note VU#333628<br>There is a remotely exploitable vulnerability in a general buffer management function in versions of OpenSSH prior to 3.7.1. This may allow a remote attacker to corrupt heap memory, which could cause a denial-of-service condition. It may also be possible for an attacker to execute arbitrary code. | |
| CVE-2003-0695 | OpenSSH 3.7.0 Buffer Overflow | CVE-2003-0695<br>Multiple "buffer management errors" in OpenSSH before 3.7.1 may allow attackers to cause a denial of service or execute arbitrary code using (1) buffer_init in buffer.c, (2) buffer_free in buffer.c, or (3) a separate function in channels.c, a different vulnerability than CVE-2003-0693. | |
| CVE-2004-2761 | IETF X.509 Certificate Signature Collision Vulnerability | CVE-2004-2761<br>US-CERT Vulnerability Note VU#836068<br>Weaknesses in the MD5 algorithm allow collisions in output. As a result, attackers can generate cryptographic tokens or other data that illegitimately appear to be authentic. | NOW Site: Bug 397514<br>Workaround available to use third-party certificate. |
| CVE-2005-2969 | SSLv2 Active | CVE-2005-2969<br>OpenSSL Advisory 20051011<br>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 SSL capabilities between system and browser. | NOW Site Bug 172506<br>Disable SSLv2. |
| CVE-2006-0225 | SCP in OpenSSH | CVE-2006-0225<br>scp in OpenSSH 4.2p1 allows attackers to execute arbitrary commands via file names that contain shell metacharacters or spaces, which are expanded twice. | NOW Site Bug 415006<br>False positive in 7.3.x. |

| CVE | Title | Description | Determination |
|---|---|---|---|
| CVE-2006-4924 | SSHv1 Vulnerability | CVE-2006-4924<br>sshd in OpenSSH before 4.4, when using the version 1 SSH protocol, allows remote attackers to cause a denial of service (CPU consumption) via an SSH packet that contains duplicate blocks, which is not properly handled by the CRC compensation attack detector. | NOW Site Bug 225733<br>Disable SSHv1. |
| CVE-2006-5051 | OpenSSH: GSSAPI DoS | CVE-2006-5051<br>Signal handler race condition in OpenSSH before 4.4 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code if GSSAPI authentication is enabled via unspecified vectors that lead to a double-free condition. | NOW Site Bug 225741<br>False positive in 7.3.x. |
| CVE-2008-1483 | OpenSSH: X11 Hijack | CVE-2008-1483<br>OpenSSH 4.3p2 and probably other versions allow local users to hijack forwarded X connections by causing ssh to set DISPLAY to:10, even when another process is listening on the associated port, as demonstrated by opening TCP port 6010 (IPv4) and sniffing a cookie sent by Emacs. | NOW Site Bug 424119<br>False positive in 7.3.x. |
| CVE-2009-3555 | SSL Renegotiation Feature | CVE-2009-3555<br>US-CERT Vulnerability Note VU#120541<br>The Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols are commonly used to provide authentication, encryption, integrity, and nonrepudiation services to network applications such as HTTP, IMAP, POP3, and LDAP. There is a vulnerability in the way that SSL and TLS protocols allow renegotiation requests that may allow an attacker to inject plain text into an application protocol stream. | NOW Site Bug 386217<br>Mitigated in Data ONTAP 7.3.3/7.3.4. |

### REPORTING A SUSPECTED SECURITY VULNERABILITY TO NETAPP

If you have an output report from a security scanner, please make sure it includes CVE numbers associated with the results before sending it to us. In general, NetApp requires reproduction information (scripts or executables) to assess the applicability of issues to its products and to create fixes or mitigations for the issues. Any assistance the scanner vendor can give in reproduction is invaluable. We need to know the name of the scanner vendor, the scanner's revision level, and the test number or CVE at a minimum, as well as the release version and configuration details of the NetApp product(s) against which the scanner was executed. Refer to the NetApp Support site for updated lists and processes: http://now.netapp.com/NOW/knowledge/docs/olio/scanner_results.

# 5 IMPLEMENT STRONG ACCESS-CONTROL MEASURES

## REQUIREMENT 8: ASSIGN A UNIQUE ID TO EACH PERSON WITH COMPUTER ACCESS

Requirement 8 of the PCI-DSS version 2 standard states:

Assigning a unique identification (ID) to each person with access ensures that each individual is uniquely accountable for his or her actions. When such accountability is in place, actions taken on critical data and systems are performed by, and can be traced to, known and authorized users.

Note: These requirements are applicable for all accounts, including point-of-sale accounts, with administrative capabilities and all accounts used to view or access cardholder data or to access systems with cardholder data. However, Requirements 8.1, 8.2 and 8.5.8 through 8.5.15 are not intended to apply to user accounts within a point-of-sale payment application that only have access to one card number at a time in order to facilitate a single transaction (such as cashier accounts).

Following is a list of settings for the password attributes for Data ONTAP.

**Table 5) Data ONTAP password attributes.**

| Rule | Default | Recommended | Setting / CLI Command |
|---|---|---|---|
| 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 1` |
| 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 attempts | 6 attempts | `options security.passwd.lockout.numtries 6` |
| Change on 1st Logon | Off | On | `options security.passwd.firstlogin.enable on` |

## REQUIREMENT 9: RESTRICT PHYSICAL ACCESS TO CARDHOLDER DATA

Requirement 9.10 of the PCI-DSS version 2 standard states:

Destroy media when it is no longer needed for business or legal reasons as follows:

- Shred, incinerate, or pulp hardcopy materials so that cardholder data cannot be reconstructed.

- Render cardholder data on electronic media unrecoverable so that cardholder data cannot be reconstructed.

This requirement can be met through the use of off-box data encryption, NetApp Storage Encryption (NSE), or by using the Disk Sanitization process built in to the Data ONTAP operating system. The Disk Sanitization process will overwrite the addressable areas of a disk that is in the spares pool. A single cycle consists of three overwrite phases. If the **`disk sanitize`** command is invoked without any switches, the first phase will write a 0x55 (U); the second phase will write a 0xaa (a); and the final phase will write a 0x3c (<). These patterns can be modified by using the full command with all of its switches:

```
disk sanitize start -p 0x26 –p 0x7e –r -c 3
```

In the above command:

- The first phase will write a hex 0x26 (&).
- The second phase will write a hex 0x7e (~).
- The third phase will write random characters.
- This will be repeated for three cycles.

**Note:** If you are using NSE (NetApp storage encryption) there is a `sanitize` command as well as a `destroy` command.

# 6 REGULARLY MONITOR AND TEST NETWORKS

## REQUIREMENT 10: TRACK AND MONITOR ALL ACCESS TO NETWORK RESOURCES AND CARDHOLDER DATA

Requirement 10 of the PCI-DSS version 2 standard states:

Logging mechanisms and the ability to track user activities are critical in preventing, detecting, or minimizing the impact of a data compromise. The presence of logs in all environments allows thorough tracking, alerting, and analysis when something does go wrong. Determining the cause of a compromise is very difficult, if not impossible, without system activity logs.

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 System Manager, are logged. All login 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

Default locations for some of the logs that are part of Data ONTAP 7G / 7-Mode are listed in the following table.

**Table 6) Data ONTAP audit logs and default locations.**

| Log | Location (File Name) |
|---|---|
| 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 |
| CIFS evt (saved) log | etc/log/adtlog.<date time stamp>.evt |
| 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 |

# 7 APPENDIX A: ADDITIONAL PCI-DSS REQUIREMENTS FOR SHARED HOSTING PROVIDERS

Requirement A.1.2 of the PCI-DSS version 2 standard states:

Restrict each entity’s access and privileges to own cardholder data environment only.

Due to the design of MultiStore, each vFiler® unit operates in its own partitioned space. Refer to the white paper NetApp MultiStore: An Independent Security Analysis.

A.1.2.d and A.1.3 discuss the logging and auditing requirements. Data ONTAP uses a centralized log for system configuration and management of the storage system. It is the responsibility of the service provider to parse and provide the events recorded in the logs to his or her clients.

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

NetApp®
www.netapp.com