Technical Report

Security Guidelines for Data ONTAP 8.0 7-Mode

Ron Demery, NetApp

February 2010 | TR-3834

ABSTRACT

This document provides guidelines and information for administering and implementing the Data ONTAP® 8.0.0 7-Mode operating system. 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. 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

1 INTRODUCTION

Confidentiality, integrity and availability: These three words sum up the intangible thing that is called “IT security.” Why is it intangible? IT security is only relevant to stakeholders because everyone does not share the same vision of security. Often, within the same organization, there can be strife concerning “security.” All of us do not see the landscape through the same set of eyes nor from the same perspective. A risk-reduced environment can be obtained only through cooperation and an understanding of the risk that an organization faces. The determination of risk that an organization sees as relevant is abstracted from an understanding of the business landscape and, therefore, is mutually exclusive to each entity. Mitigation of this risk can be *de jure* (by law or standards) or *de facto* (common accepted practice) and is always situational.

Most of the recommendations made within this document are *de facto* in nature. It would be rather presumptuous of us to claim knowledge of your security posture.

2 STORAGE CONTROLLER DEFAULTS

Data ONTAP is an operating system that provides file services (NAS) as well as block services (SAN). As with any operating system, care must be taken with the granting of administrative access to the hardware that is controlled by the operating system. This includes both logical as well as physical access.

2.1 CLEAN INSTALL VERSUS UPGRADE

The default settings apply only to storage systems shipped with Data ONTAP 8.0 or later. For storage systems upgraded from an earlier version of Data ONTAP to Data ONTAP 8.0 or later, the default settings do not apply. Instead, for those upgraded systems, the settings remain unchanged after the upgrade. Also, if you make security setting modifications after upgrading to Data ONTAP 8.0 or later, the modifications are preserved even if the system reverts back to the previous Data ONTAP version.

2.2 DEFAULT PASSWORD SETTINGS AND RECOMMENDATIONS

When this operating system is initialized (not upgraded from a previous version of Data ONTAP) there is a single account. During the setup of Data ONTAP you will be required to supply a password for the `root` account. The password must be eight characters in length and contain a minimum of two alpha characters and one numeric character. A password with a minimum of eight characters on the `root` account is required if you wish to use snmpv3

PASSWORD DEFAULT SETTINGS AND RECOMMENDATIONS

Table 1 contains the recommendations for the password properties. The “Data ONTAP 8.0 7-Mode 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 1) Local storage system password attributes.

Rule	Default	Recommended	Setting / cli command
Root Access	On	Off	`options security.passwd.rootaccess.enable on`
Apply to All Accounts	On	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	6	`options security.passwd.rules.minimum.alphabetic 6`

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 attempts	6 attempts	`options security.passwd.lockout.numtries 6`
Change on 1st Logon	Off	On	`options security.passwd.firstlogin.enable on`

Recommendations: If you are upgrading from an earlier version of Data ONTAP, ensure that you applied a password to the `root` account and apply the settings in Table 1.

2.3 LOCAL ACCOUNT AGING

Data ONTAP provides the ability to set the account aging limits on each local account upon creation of the account. This provides flexibility to the security administration of the storage system. To set the minimum age of the account you would use the `-m` option with the `useradmin user` or the `useradmin user modify` commands. To set the maximum age or the account you would use the `-M` option with the `useradmin user add` or the `useradmin user modify` commands.

The `-m` option specifies the minimum allowable age of the user's password (in days) before the user can change it again. This works in conjunction with the option `security.passwd.rules.history` to make sure that users have unique, nonrepeating passwords.

The `-M` option specifies the maximum allowable age of the user's password (in days). When the user's password expires, the user's status is set to "Password Expired" and the user can only run the `passwd` command.

Examples:

```
useradmin user add <newuser> -g <group1, group2, ..> -m 1 -M 90
```

```
useradmin user modify <olduser> -g <group1, ...> -m 1 -M 90
```

Note: Before using the password minimum age feature, make sure your storage system time is set correctly. Changing the system time after password minimum ages have been set can lead to unexpected results.

For detailed information on user account management, please refer to the "How to manage administrator and diagnostic access" section of the "Data ONTAP 8.0 7-Mode System Administration Guide."

2.4 DEFAULT SERVICE ATTRIBUTES

On storage systems shipped with Data ONTAP 8.0 or later, secure protocols are enabled and nonsecure protocols are disabled by default. SecureAdmin is set up automatically on storage systems shipped with Data ONTAP 8.0 or later. For these systems, the following are the default security settings:

- Secure protocols (including SSH, SSL, and HTTPS) are enabled by default.
- Nonsecure protocols (including RSH, Telnet, FTP, and HTTP) are disabled by default.

Table 2) default storage system services

Service	Default State
File Transfer Protocol (FTP)	Off
FilerView® https://<filer_IP>/na_admin (httpd.admin.ssl.enable)	On
Network Data Management Protocol (NDMP)	Off
Remote Shell (rsh)	Off
RIP – routed	On
Secure Shell (ssh)	On
Secure Sockets Layer (SSL) v2 and V3	On
Simple Network Management Protocol (SNMP)	On
Telnet	Off
Trivial File Transfer Protocol (TFTP)	Off

For a more detailed discussion, please refer to the “Secure protocols and storage system access” section of the “Data ONTAP 8.0 7-Mode System Administration Guide.”

2.5 SERIAL PORT ACCESS (LOCAL ADMINISTRATION)

The console port is the initial entry point into the storage system for administration and initialization. The term “Local Administration” is used loosely; if you have many storage systems they are likely to have their serial ports connected to a terminal server. In order to access the storage system through the console port the user account must have `login-console` capability. This capability is assigned, by default, to the `root` account and the `Administrators` group.

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

Recommendation: Set the timeout value to 10 minutes.

2.6 AUDIT LOGGING

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, 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 was 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

You can access the audit-log files using your NFS or CIFS client, or using HTTP.

For detailed information on audit logging and its capabilities, please refer to the “Audit logging” section of the “Data ONTAP 8.0 7-Mode System Administration Guide.”

2.7 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. This is accomplished through the use of the `useradmin` command at the storage system cli.

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, Data ONTAP requires that you specify a group membership. It is a best practice to create appropriate groups before creating local 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 8.0 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 command-line interface.
- Compliance rights: These capabilities provide the ability to execute compliance-related operations.
- FilerView right: This right grants read-only access to FilerView.
- Log-in 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 "How to manage administrator and diagnostic access" section of the “Data ONTAP 8.0 7-Mode System Administration Guide.”

Recommendation: Use care when assigning local users or “domain users” to the `Administrators` group, the `Compliance Administrators` group, or the `Power Users` group on the storage system. Each of those groups has the authorization to modify the configuration of the storage system.

Note: In order to add a “domain user” to a group in the storage systems local account database, a CIFS protocol license is required.

2.8 ADMINISTRATIVE AUTHENTICATION LOCAL VERSUS REMOTE

Data ONTAP provides the option to use an external LDAP-based authentication repository. This option is controlled by the `security.admin.authentication` option setting. The default value for this option is internal. This option controls where the storage finds authentication information for admins. Authentication can be done via the local administrative repository or through repositories found in the `nsswitch.conf` file. Authentication via `nsswitch.conf` allows ldap and nis centralized administration. The value of this option can be ‘internal,’ ‘nsswitch,’ ‘internal,nsswitch,’ or ‘nsswitch,internal.’ The repositories are searched in the order specified.

Recommendation: Use only local accounts for administrative functions.

3 REMOTE ADMINISTRATION

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: Use this card to connect to a TCP/IP network to administer the storage system:

- From any client by using a Web browser and the FilerView interface
- 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 RLM or BMC maintenance port that is part of the storage system:

- From any client by using a Secure Shell client application, such as SSH, OpenSSH for UNIX® hosts, or PuTTY for Windows hosts

3.1 FILERVIEW

Provides access via port 80/443. It is available on all platforms.

You can use FilerView to access a storage system. FilerView is an HTTP/Web-based graphical management interface that enables you to manage most storage system functions from a Web browser rather than by entering commands at the console, through a Telnet session, the `rsh` command, or by using scripts or configuration files. You can also use FilerView 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. You can also view statistics about network traffic. FilerView online Help explains Data ONTAP features and how to use them. FilerView supports Internet Explorer version 6.0 and Firefox version 2.0.

The following options control access to FilerView:

- `httpd.admin.access`: (Off by default) Restricts HTTP access to FilerView. If this value is set, `trusted.hosts` is ignored for FilerView access.
  - 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`: (Off by default) Enables HTTP access to FilerView.
- `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.
  - 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.
- `httpd.admin.ssl.enable`: (On by default) Enables HTTPS access to FilerView.
- `httpd.admin.top-page.authentication`: (On by default) Specifies whether the top-level FilerView administration Web page prompts for user authentication.
  - Setting this option to Off allows access to the man pages without the need to log on to the storage system. It is still necessary to provide valid credentials when selecting the FilerView or the Filer-at-a-Glance icons to perform actions on the storage system.

3.2 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 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 or 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 On.

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 8.0 7-Mode System Administration Guide."

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

Recommendations: If Telnet is used, set the session timeout to a value of 5 minutes and take precautions to ensure that the accounts and passwords are not compromised in transit from the client to the storage controller. Set a banner message through the creation of the `/etc/issue` file.

For detailed information on Telnet and its capabilities, please refer to the "Telnet sessions and storage system access" section of the "Data ONTAP 8.0 7-Mode System Administration Guide."

3.3 RSH

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

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

For detailed information on RSH and its capabilities, please refer to the "How to access a storage system using a Remote Shell connection" section of the "Data ONTAP 8.0 7-Mode System Administration Guide."

3.4 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 8.0 7-Mode System Administration Guide."

Recommendation: Ensure that ssh1 is disabled; only ssh2 is enabled by default. Then check the status of ssh and ssl using the `secureadmin status` command at the storage system cli.

The ssh session timeout is defaulted to 600 seconds (10 minutes).

Recommendation: Set the options `ssh.idle.timeout` to a value of 300 (5 minutes).

The `telnet.distinct.enable` option enables making the ssh and console separate user environments.

Recommendation: Set the `telnet.distinct.enable` option to On.

For detailed information on SSH and its capabilities, please refer to the “SSH protocol” section of the “Data ONTAP 8.0 7-Mode System Administration Guide.”

For detailed information on the `secureadmin` command, please refer to the “secureadmin” section of the “Data ONTAP 8.0 7-Mode Commands: Manual Page Reference,” Volume 1.

3.5 RLM PORT ACCESS

The RLM command line interface (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. This is available on the 3xxx and 6xxx series platforms.

Determine that the RLM firmware is version 4 or above. In version 4 firmware only ssh2 is enabled. The ssh protocol on the RLM is part of the RLM’s kernel operating system and therefore segmented for the implementation of ssh by the Data ONTAP operating system.

Recommendation: Disable the `root` account and utilize accounts that are members of the storage systems `Administrators` group to manage the storage system through the RLM.

Note: The RLM ignores the `ssh.idle.timeout` option and the `console.timeout` option. The settings for these options do not have any effect on the RLM.

For detailed information on the RLM and its capabilities, please refer to the “The Remote LAN Module” section of the “Data ONTAP 8.0 7-Mode System Administration Guide.”

3.6 BMC PORT ACCESS

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.

Available on the 2040 platform only (for Data ONTAP 8.0), BMC requires the SSH client and uses the root password. It shares the active console session if one is active when the `system console` command is issued from the `bmc shell` prompt.

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.

Note: The BMC ignores the `ssh.idle.timeout` option and the `console.timeout` option. The settings for these options do not have any 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.

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 via SSH, you must configure the Data ONTAP root password. BMC accepts passwords that are no more than 16 characters.

Recommendation: Take great care when using the BMC Management Port on the storage system. Set a strong password on the `root` account, disable the `root` account, and reset the root password on a regular basis.

For detailed information on the BMC and its capabilities, please refer to the “The Baseboard Management Controller” section of the “Data ONTAP 8.0 7-Mode System Administration Guide.”

3.7 SNMP

SNMP is enabled by default in Data ONTAP. SNMP managers can query your storage system's SNMP agent for information. The SNMP agent gathers information and forwards it to the managers by using SNMP. The SNMP agent also generates trap notifications whenever specific events occur.

For diagnostic and other network management services, Data ONTAP provides an SNMP agent compatible with SNMP versions 1, 2c, and 3. SNMP v3 offers advanced security by using pass phrases and encryption. SNMP v3 supports the MIB-II specification and the MIBs of your storage system.

Recommendation: Use SNMP v3.

In order to enable SNMP v3 it is necessary to add a local group to the storage controller that has `login-snmp` capability. Then add the local user account to the group. These steps are outlined in the “Network Management Guide for Data ONTAP 8.0 7-Mode” in the “Configuring SNMP v3 users” section.

Note: SNMP does not support “domainuser” authentication. The authentication account for SNMP must be an account that is local to the storage system.

3.8 LOG-ON BANNERS

Once created, the `/etc/motd` file provides a banner to be displayed on the lower page of the FilerView entry page. The `/etc/motd` file is not present on the storage system by default. This also provides a post-log-in message to the cli authentication process.

Once created the `/etc/issue` file provides a pre-log-in message to be displayed at the cli prompt.

Note: The `/etc/motd` file and 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 8.0 7-Mode System Administration Guide.”

Recommendation: Create and maintain the `/etc/issue` and the `/etc/motd` files on your storage systems.

4 PORT SCANNING

Data ONTAP operating system software for NetApp storage systems optimizes serving data by combining patented file system technology and a microkernel design dedicated to multiprotocol data access.

While CIFS is one of the protocols for data access supported by Data ONTAP, NetApp storage systems are not Microsoft® servers. As a result, NetApp does not respond to imputed vulnerabilities identified by third-party vulnerability scanners when a NetApp storage system is misidentified as a Windows server.

The versions of OpenSSH (and OpenSSL) code incorporated into Data ONTAP have to be declared using the version string from which they were originally derived according to the licensing agreements. The code has, however, been heavily customized for use in Data ONTAP and we apply the patches that are deemed to be applicable to our implementations.

Scanners that react only to the version string rather than testing for the vulnerability are always going to be inaccurate.

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.

4.1 WELL-KNOWN PORTS

Although some port scanners are able to identify storage systems as storage systems, other port scanners report storage systems as unknown types or as UNIX systems because of their NFS support or as Windows

systems because of their CIFS support. There are several services that are not currently listed in the `/etc/services` file.

Table 3 is a sample output of the `/etc/services` file.

Table 3) Sample `/etc/services` file output.

Service	Port/Protocol	Description
ftp-data	20/tcp	
ftp	21/tcp	
ssh	22/tcp	
telnet	23/tcp	
smtp	25/tcp	
time	37/tcp	Time service
time	37/udp	
domain	53/udp	
domain	53/tcp	
portmap	111/udp	
portmap	111/tcp	
dhcps	67/udp	DHCP server
dhcpc	68/udp	DHCP client
tftp	69/udp	
http	80/tcp	
Kerberos	88/udp	Kerberos 5
Kerberos	88/tcp	Kerberos 5
nntp	119/tcp	
ntp	123/tcp	Network Time Protocol
ntp	123/udp	Network Time Protocol
netbios-name	137/udp	NetBIOS nameserver
netbios-dg	138/udp	NetBIOS datagram service
netbios-ssn	139/tcp	NetBIOS service session
snmp	161/udp	
ldap	389/tcp	LDAP session
https	443/tcp	SecureAdmin/SSL
cifs-tcp	445/tcp	CIFS over TCP with NetBIOS framing
kpasswd	464/tcp	Appliance does not listen on this port; used as Domain Controller destination port for Kerberos passwd set/change operations
shell	514/tcp	
syslog	514/udp	
route	520/udp	
ldap-ssl	636/tcp	LDAP over SSL
kerberos-sec	750/udp	For compatibility with older "750" clients
kerberos-sec	750/tcp	For compatibility with older "750" clients
nfsd	2049/udp	
nfsd	2049/tcp	
nrv	2050/tcp	NetApp Remote Volume protocol, used in FlexCache® and Restore on Demand
iscsi-target	3260/tcp	
nlockmgr	4045/tcp	NLM
nlockmgr	4045/udp	
mountd	4046/tcp	NFS mountd protocol
mountd	4046/udp	
status	4047/tcp	
status	4047/udp	
pcnfsd	4048/tcp	PCNFS protocol
pcnfsd	4048/udp	
rquotad	4049/udp	
ndmp	10000/tcp	
sm-ics	10565/tcp	SnapMirror® multipath
snapmirror	10566/tcp	
sm-sync-block	10567/tcp	SnapMirror Sync block data
sm-sync-trans	10568/tcp	SnapMirror Sync transaction data

Service	Port/Protocol	Description
sm-sync-ctrl	10569/tcp	SnapMirror Sync control data
nbu-nearstore	10571/tcp	NetBackup™ – NearStore®

Many other open ports may show up in a report from a utility such as the `netstat` command from the cli. For further information on IP port usage for the operating system, refer to the "IP port usage on a storage system" section of the "Data ONTAP 8.0 7-Mode Network Management Guide."

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 with 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 SnapMirror protocol can be found in the following references:

"Data ONTAP 8.0 7-Mode 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 8.0 7-Mode 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 8.0 7-Mode 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 provides support (license required) for the CIFS protocol, which is documented in an Internet Engineering Task Force (IETF) Internet 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 8.0 7-Mode 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)

5.5 NFS

The appliance supports versions 2, 3, and 4 of the NFS protocol, which are documented in RFC’s 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 pathname on a server to an NFS filehandle 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 8.0 7-Mode 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.

www.netapp.com