Technical Report

Data ONTAP Security Guidance

Ron Demery, CISSP, NetApp

August 2012 | TR-3950

Data ONTAP 8.1.1 Operating in 7-Mode

This paper focuses on the administrative data path to the Data ONTAP® 8.1.1 operating system operating in 7-Mode. In it we discuss the access methods, identification, and authentication of the local accounts and audit logging. This report contains recommendations and best practices for the security-minded storage administrator.

TABLE OF CONTENTS

1 Overview ... 4

1.1 Know Your Environment ... 4

1.2 Know Your Data ... 4

1.3 Know Your People ... 4

1.4 Know Your Exposure ... 5

2 Security Features Added in Data ONTAP 8.1 Operating in 7-Mode ... 5

3 Storage Controller Defaults ... 5

3.1 Clean Install Versus Upgrade ... 5

4 Secure System Defaults ... 5

4.1 Enable Secure Administrative Access ... 6

4.2 Disable Unnecessary Services ... 9

5 Default Accounts ... 10

5.1 root account ... 10

5.2 diag account ... 10

5.3 Default Password Settings and Recommendations ... 10

5.4 SNMP ... 11

6 Management Paths ... 12

6.1 Storage System (Hardware) Management ... 12

6.2 Data ONTAP (Software) Management ... 16

6.3 Role-Based Access Control (RBAC) ... 18

7 Integration with Active Directory Authentication ... 19

8 Integration with LDAP/NIS Authentication ... 20

8.1 LDAP ... 20

8.2 NIS ... 21

9 AutoSupport ... 21

10 Audit Logging ... 22

11 Firewalling and Protocol Access Controls ... 23

11.1 Protocol Blocking (Firewalling) ... 23

11.2 Protocol Access Filters ... 23

12 Vulnerability Scanners and Reporting ... 24

12.1 Reporting Suspected Vulnerabilities ... 24

Appendixes 24

Log-on Banners 24

Maximums 24

Data ONTAP Log Locations 26

CIFS Protocol 27

NFS Protocol 28

Secure File Transfer Protocol 28

MultiStore 28

References / Links 30

Version History 30

LIST OF TABLES

Table 1) Data ONTAP services and their default state 5

Table 2) Options that control SSH connections after setup. 7

Table 3) Options that control SSL after setup (Data ONTAP 8.1.0 7-Mode). 8

Table 4) Options that control System Manager / SDK connections. 9

Table 5) Nonsecure services and their default states. 9

Table 6) Data ONTAP password defaults and recommendations. 11

Table 7) BMC summary. 13

Table 8) SP summary. 13

Table 9) New options in SP FW 2.1. 14

Table 10) RLM summary. 15

Table 11) New options in RLM FW 4.1 15

Table 12) Data ONTAP maximums. 24

Table 13) Data ONTAP log locations. 26

1 Overview

What exactly is security? Is it an avoidance of risk? If so, who defines the acceptable risk level? Is it the CIO, a law, a standard, a compliance doctrine, a government-imposed regulation?

In the past several years we have seen the outer boundaries or the outer shell of IT security shrink. We are no longer just concerned with the network, servers, and desktop systems. Unless you have been sleeping, you have probably noticed your customers' desire/demand to use their smartphones, tablets, and other consumer computer devices to access the network. There is also the move to shared storage infrastructures or cloud services. Whether these services are infrastructure as a service (IaaS), platform as a service (PaaS), software as a service (SaaS), private, or public, the storage layer is a vital component. With the emergence of the Cloud Security Alliance Control Matrix, NERC, PCI-DSS, EMEA data privacy policies, and other governance, risk, and compliance (GRC) concerns, we as storage administrators need to let IT auditors know that we have the proper controls in place to meet their concerns. Do we have the proper IT controls and audit logging in place?

1.1 Know Your Environment

How many user data paths are there to your storage system? How many administrative data paths are active to access your system? Which paths can share the infrastructure—physical as well as logical? Do you know where your bits have been? Is your cold iron documented—in other words, do you have an infrastructure diagram with enough detail to rebuild the infrastructure if required? Is it current? Is your storage configuration documented? Do you have a standard configuration for your storage? How good is your change control—does it really work?

These questions are a few of those that must be answered in order to know your environment, and answering them can be a daunting task for the new storage architect or administrator. Rely on the corporate knowledge of the networking, server, and application teams. It is necessary for everyone to work together to keep the data available and the customers happy.

1.2 Know Your Data

Because the paranoid population fears the cloud architecture, it will become increasingly important to provide assurances as to the boundaries in which a customer's data is stored. This is especially true for SaaS implementations. It also comes into play with several laws that require that certain types of data do not cross a national boundary. Customers may also start to require that their cloud service provider (CSP) assure them about where their data is stored. This will all be sorted out in the terms and conditions of the contract between the CSP and the customer. It was also a major topic for discussion at many of the recent security conferences.

1.3 Know Your People

Who has administrative access to the storage system? What is their role? Did corporate run a background check, and, if so, was it local or national? What hours do these people normally work? Is their account in use at odd hours? How do you know that—do you log and review the administrative access and system configuration changes? Do you log data access to the user data (success and failure), and is it important? What are the e-discovery requirements to which you must adhere? Just because an account holder has access to a datastore, does he/she normally visit it?

1.4 Know Your Exposure

Do you proactively scan your infrastructure with a port or vulnerability scanner? Do you actually analyze the results at each device or just file the reports? Do you work with the IT Security Team to educate them on the storage system operating system? Do they understand SAN versus NAS versus administrative ports? Is mass data deletion or movement expected/flagged/tracked/logged?

2 Security Features Added in Data ONTAP 8.1 Operating in 7-Mode

TLS, SFTP, and FTPs were added to the security feature set in Data ONTAP 8.1 7-Mode. These features are not available in Data ONTAP 8.0.x 7-Mode.

3 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 and physical access.

3.1 Clean Install Versus Upgrade

The default settings apply only to storage systems shipped with Data ONTAP 8.1 or later. For storage systems upgraded from an earlier version of Data ONTAP to Data ONTAP 8.1 or later, the default settings do not apply except to previously unavailable settings. For upgraded systems, the settings remain unchanged after the upgrade. Also, if you make security setting modifications after upgrading to Data ONTAP 8.1 or later, the modifications are preserved even if the system reverts to the previous Data ONTAP installation, unless they did not exist in the previous installation, in which case they will be ignored. Please note that if a setting was expanded (such as ACEs on ACLs) during an upgrade, the results could be unpredictable after a revert.

4 Secure System Defaults

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.

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

Table 1) Data ONTAP services and their default state.

Service	Default State Data ONTAP 8.1.0 7-Mode
File Transfer Protocol (FTP)	Off
Secure File Transfer Protocol (SFTP)	Off
File Transfer Protocol over SSL (FTPS)	Off
HTTP	Off
httpd.admin.ssl.enable (used for System Manager / SDK access)	On

Service	Default State Data ONTAP 8.1.0 7-Mode
httpd.admin.enable (used for System Manager / SDK Access)	Off
Network Data Management Protocol (NDMP)	Off
Remote Shell (rsh)	Off
RIP – routed (RIPv1)	On
Secure Shell Service (ssh)	On
Secure Shell v1 (SSHv1)	Off
Secure Shell v2 (SSHv2)	On
Secure Sockets Service (SSL)	On
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	Off
Transport Layer Security v1 (TLSv1)	Off
Trivial File Transfer Protocol (TFTP)	Off
WebDav	On

4.1 Enable Secure Administrative Access

NetApp recommends that you configure and enable SecureAdmin™ software 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. SSH public keys provide a stronger and more granular method of SSH access to NetApp storage systems.

Setting Up SSH

SSH is enabled by invoking the **secureadmin setup ssh** command at the CLI or through System Manager under <storage controller name> => Configuration => Security => SSH/SSL.

```
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`**
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`**

Option	Default	Recommended	Setting / cli Command
telnet.distinct.enable	On	On	Enables making the ssh and the 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.

Data ONTAP supports SSLv2 and SSLv3. You should use SSLv3 or TLS because they offer better security protections than those of previous SSL versions.

Note: In Data ONTAP version 7.3.4 the option to disable SSLv2 (options ssl.v2.enable off) was added.

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 Open SSL Vulnerability CVE-2009-3555," for further details.

SSL is enabled by invoking the `secureadmin setup ssl` command at the CLI or through System Manager under <storage controller name> => Configuration => Security => SSH/SSL.

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 8.1.0 7-Mode).

Option	Default	Recommended	Setting / cli Command
ssl.enable	On	On	**`options ssl.enable on`**
ssl.v2.enable	On	Off	**`options ssl.v2.enable off`**

Option	Default	Recommended	Setting / cli Command
ssl.v3.enable	On	On	`options ssl.v3.enable on`
tls.enable	Off	On	`options tls.enable on`

Enabling SSL for System Manager

By default, System Manager will attempt a connection using ssl; if this is not available it will ask if you wish to continue using clear text. NetApp recommends that the ssl protocol be utilized for all api / 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 System Manager.

Table 4) Options that control System Manager / SDK connections.

Option	Default	Recommended	Setting / cli Command
httpd.admin.enable	Off	Off	`options httpd.admin.enable off`
httpd.admin.ssl.enable	On	On	`options httpd.admin.ssl.enable on`

4.2 Disable Unnecessary Services

By default, telnet, RIPv1, rsh, and webdav are disabled. 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 host=-` Refer to the Manual Page Reference, Volume 2 - na_protocolaccess(8), for valid values.
rsh.enable	Off	Off	`options rsh.enable off`
telnet.access	legacy	Host or None	`options telnet.access host=-` Refer to the Manual Page Reference, Volume 2 - na_protocolaccess(8), for valid values.
telnet.distinct.enable	On	On	`options telnet.distinct.enable on` This option also affects the SSH interactive sessions.
telnet.enable	Off	Off	`options telnet.enable off`
webdav.enable	On	Off	`options webdav.enable off`
Routed	On	Off	RIPv1 port 520 is not authenticated. `routed off`

5 Default Accounts

Many of the current governance, risk, and compliance (GRC) standards require that all default accounts be locked or disabled. The default accounts for the Data ONTAP 8.1.1 7-Mode operating system are root, diag, and SNMP.

5.1 root account

Always check with the administrators of the host-based services about which of them may be using the root account. These could be SnapDrive® technology, SnapManager® for Virtual Interface, DataFabric® Manager, or one of the Host Attach Kits (HAKs), among others. If the administrators are using root they will be adversely affected when you disable the account. Work with the administrators to create a proper service account (new account) for the application and assign the new account the proper capabilities or predefined role.

Best Practice

Create a new storage administrator account and assign it to the Administrators group.

```
useradmin user add stgAdmin -g Administrators -m 1 -M 90
```

Disable `root`.

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

5.2 diag account

A diagnostic account, named “diag,” is provided with your storage system. You can enable the diagnostic account to perform troubleshooting tasks in the system shell. The diagnostic account and the system shell are intended only for low-level diagnostic purposes and should be used only with guidance from Technical Support. The default state for this account is disabled.

The password requirements for diag are:

- Minimum 8 characters
- Contain at least 1 letter and 1 number
- History = 6

Best Practice

Keep the diag account disabled when not in use.

```
priv set advanced
useradmin diaguser lock
useradmin diaguser show
```

Reset the password on every use.

```
priv set advanced
useradmin diaguser password
```

5.3 Default Password Settings and Recommendations

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. Note that the boot menu password reset capability has a more limited set of valid password criteria than the runtime Data ONTAP criteria. If a password is changed using the boot menu, it should be changed again after completing the boot process so that it conforms to all expectations.

Table 6) Data ONTAP password defaults and recommendations.

Rule	Default	Recommended	Setting / cli command
Root Access	On	Off (after creation of a local equivalent)	`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	256	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`

Note: The default settings apply only to storage systems shipped with Data ONTAP 8.1.1 7-Mode. For storage systems upgraded from an earlier version of Data ONTAP 7G to Data ONTAP 8.1.1 7-Mode, the default settings do not apply. Instead, for those upgraded systems, the settings remain unchanged after the upgrade.

5.4 SNMP

SNMP is enabled by default in Data ONTAP. SNMP managers can query their 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.

Best Pratice

Disable SNMPv1/2c

```
toaster>snmp community delete all
```

Use SNMPv3.

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 8.1.1 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.

6 Management Paths

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
- Any configured Ethernet port

6.1 Storage System (Hardware) Management

All NetApp FAS storage systems provide an out-of-band management port for the maintenance and management of the storage system hardware. These IP-based ports provide communications via SSH for interactive session confidentiality.

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.

Available on the FAS2040 platform only (for Data ONTAP 8.1), BMC requires an 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.

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, please refer to the “Using the Baseboard Management Controller for remote system management” section of the “Data ONTAP 8.1.1 7-Mode 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 via SSH, you must configure the Data ONTAP `root` password. BMC accepts passwords that are no more than 16 characters.

Table 7) 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
```

Service Processor (SP)

The SP command line interface (CLI) commands enable you to remotely access and administer the storage system and diagnose error conditions. Also, the SP extends AutoSupport™ tool 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 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.

SP firmware 2.1 added the functionality to restrict host access and disconnect idle connections.

For detailed information on the SP and its capabilities, please refer to the “Using the service processor for remote system management” section of the “Data ONTAP 8.1.1 7-Mode System Administration Guide.”

Table 8) SP summary.

Storage Systems	Connection Protocol	Current Firmware	Idle Connection Timeout	Failed Login IP Lockout

Storage Systems	Connection Protocol	Current Firmware	Idle Connection Timeout	Failed Login IP Lockout
FAS32xx	SSHv2	2.1	Yes	Yes
FAS62xx	SSHv2	2.1	Yes	Yes

Table 9) New options in SP FW 2.1.

Property	Description	Command Line Entry
Host access	Restricts access to a host. This can be host name IPv4 or IPv6 addresses.	**`options sp.ssh.access <host>`**
Connection timeout enable	Turns on or off (default is on).	**`options sp.autologout.enable`**
Connection timeout time	Number of minutes for disconnect of an idle session (default is 60).	**`options sp.autologout.timeout`**

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.

Determine that the FW is version 2.1 or later.

Set the idle timeout to 10 minutes or less.

Restrict host access to the SP interface.

Note: The default SP **`naroot`** account uses the Data ONTAP `root` password to allow access over the LAN with SSH. The SP interface accepts passwords that are no more than 16 characters.

Remote LAN Module (RLM)

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.

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.

RLM firmware version 4.1 added the functionality to restrict host access and provide idle session timeouts.

For detailed information on the RLM and its capabilities, please refer to the "Using the Remote LAN Module for remote system management" section of the "Data ONTAP 8.1.1 7-Mode System Administration Guide."

Note: To clear the memory of the RLM see https://kb.netapp.com/support/index?page=content&id=1011518.

Table 10) RLM summary.

Storage Systems	Connection Protocol	Current Firmware	Idle Connection Timeout	Failed Login IP Lockout
FAS30xx	SSHv2	4.1	Yes	Yes
FAS31xx	SSHv2	4.1	Yes	Yes
FAS60xx	SSHv2	4.1	Yes	Yes

Table 11) New options in RLM FW 4.1.

Property	Description	Command Line Entry
Host access	Restricts access to a host. This can be host name IPv4 or IPv6 addresses.	`options rlm.ssh.access <host>`
Connection timeout enable	Turns on or off (default is on).	`options rlm.autologout.enable`
Connection timeout time	Number of minutes for disconnect of an idle session (default is 60).	`options rlm.autologout.timeout`

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 4.1 or later.

Set the idle timeout to 10 minutes or less.

Restrict host access to the RLM interface.

Note: The default RLM **`naroot`** account uses the Data ONTAP `root` password to allow access over the LAN with SSH. The RLM interface accepts passwords that are no more than 16 characters.

6.2 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 by using System Manager
- From any client by using a telnet session (after enabling telnet, which, by default, is off)
- From any client by using a Remote Shell connection
- From any client by using a Secure Shell connection

System Manager

System Manager (a primary GUI management tool) provides access via 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 rather than by entering commands at the console, through a telnet session, the rsh command, or scripts or configuration files. 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 from the user data access path.

Set / verify the following options:

- httpd.admin.ssl.enable (On 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 (Off 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 in which 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 (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 user name 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 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 8.1.1 7-Mode System Administration Guide."

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

Best Practice

If telnet is used, set the following options.

- Distinct sessions form 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, please refer to the "Telnet sessions and storage system access" section of the "Data ONTAP 8.1.1 7-Mode System Administration Guide."

RSH

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

Recommendations

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, please refer to the "How to access a storage system using a Remote Shell connection" section of the "Data ONTAP 8.1.1 7-Mode 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 8.1.1 7-Mode System Administration Guide."

Recommendations

- Determine that ssh1 is disabled; only ssh2 is enabled by default.

  ```
  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, please refer to the "SSH protocol" section of the "Data ONTAP 8.1.1 7-Mode System Administration Guide."

For detailed information on the `secureadmin` command, please refer to the "secureadmin" section of the "Data ONTAP 8.1.1 7-Mode Commands: Manual Page Reference," Volume 1.

6.3 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 only access data stored on the NetApp storage system are not usually part of this definition.

Groups

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

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

Roles

Roles are defined as sets of capabilities. Data ONTAP comes with several predefined roles, which you can modify. You can also create new roles. 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 8.1.1 uses five 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.
- 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 NetApp technical report TR-4062.

7 Integration with Active Directory Authentication

The ability to define domain users who are authenticated by an Active Directory® (AD) domain rather than by Data ONTAP is a powerful tool for managing large storage environments. Most enterprise computing environments already have an Active Directory infrastructure available, and storage administrators and other users who need administrative access to storage devices already have accounts defined within that infrastructure. Using this preexisting authentication capability, rather than defining separate accounts for the storage environment, confers key benefits.

- An administrator’s authentication credentials (user name, password) are the same when logging into the storage system as they are when logging into any Windows system in the environment. When the password is changed in the Windows environment, the change takes effect immediately in the storage environment.
- Changing an administrator’s password once, in Active Directory, has the effect of changing it on all storage devices to which that administrator has access. This is a significant reduction in management overhead for environments with a large number of storage devices.
- Centralized authentication allows local security policy, implemented in Active Directory, to take effect across all storage devices as well. For example, administrators might be compelled to change their passwords with a certain frequency and might receive advance warning as the password expiration date approaches. Similarly, when they do change passwords, the Active Directory environment can enforce policy about password composition and length, reuse of previous passwords, use of dictionary words in passwords, and so on.
- When an administrator leaves an organization, disabling that administrator’s Active Directory account immediately revokes access to the storage environment as well.

However, it is not advisable to give *all* of the accounts in Active Directory access to storage management functions. Obviously, only a subset of the AD accounts represents administrative staff, and only a subset of the administrative staff (in a large organization) needs to administer storage controller systems. Any system that provides transparent Active Directory authentication on a storage system without discriminating between authorized administrators and other accounts exposes the storage system to huge security problems.

To avoid such problems, Data ONTAP authenticates an administrator against Active Directory only if that administrator has been defined as a domain user by using the **`useradmin`** command.

Note: By default, the Domain Admins group has the ability to manage login access to the administrative interface of Data ONTAP. This includes telnet, SSH, RSH, System Manager, and other NetApp SDK-based tools.

Best Practice

Create a domain security group in Active Directory for the accounts that require access to the Data ONTAP administrative functions (volume creation, storage system setup, and so on).

Add that Domain Security group to the Data ONTAP administrators group.

```
OntapSC> useradmin domainuser add domain\OntapAdminGrp –g administrators
```

Test the Data ONTAP administrative access for a user in the newly created Domain group.

Remove the Domain Admins group from the Data ONTAP administrators group:

```
OntapSC> useradmin domainuser delete domain\”Domain Admins” –g administrators
```

This practice can be used with other predefined groups in Data ONTAP as well as with custom groups that you create. This is handy when you are creating access for NetApp Manageability SDK or Data ONTAP PowerShell™ Toolkit applications and you don’t want to give the users or service accounts administrative access to Data ONTAP.

8 Integration with LDAP/NIS Authentication

It is possible to set up administrative authentication in conjunction with an LDAP or a NIS server. Once the connection to the LDAP / NIS server is tested, you can designate LDAP groups to have different roles for the administration of Data ONTAP. The requirements are the following.

8.1 LDAP

Set options for connection to LDAP server:

```
options ldap.base "dc=x,dc=y,dc=local"
options ldap.servers "a.z.x.y.local"
options ldap.servers.preferred "a.z.x.y.local"
options ldap.name "cn=admin,dc=x,dc=y,dc=local"
options ldap.passwd <password>
options ldap.enable on
```

Modify the /etc/nsswitch.conf for administrative identification and authentication search order:

```
passwd: ldap files nis
netgroup: ldap files nis
group: ldap files nis
```

Set options that control administrative search order:

```
options security.admin.authentication nsswitch,internal
```

This entry will cause the authentication engine to look at the nsswitch.conf file to see the order of interrogation to resolve the user name. If the user name is not resolved it will search the local Data ONTAP user database.

```
options security.admin.nsswitchgroup <ldapgrp0,ldapgrp1:power>
```

This entry defines the groups within the LDAP target container that have permissions and roles for administration within Data ONTAP. In this case the group ldapgrp0 will be mapped to the admin role, and the group ldapgrp1 will be mapped to the power role.

Test connection to the LDAP service:

Use the `getXXbyYY` command on the storage controller to verify that the appliance gets the information from the LDAP server.

Note: For further information on the configuration of the LDAP service, refer to the “Data ONTAP 8.1.1 7-Mode File System and Protocol Administrators Guide.”

8.2 NIS

Set options for connections to NIS server:

```
options nis.domainname <nis domain>
options nis.enable on
options nis.group_update_schedule    24
options nis.netgroup.domain_search.enable on
options nis.netgroup.legacy_nisdomain_search.enable on
options nis.servers <IP address>
options nis.slave.enable
```

Modify the /etc/nsswitch.conf for administrative identification and authentication search order:

```
passwd: nis files ldap
netgroup: nis files ldap
group: nis files ldap
```

Set options that control administrative search order:

```
options security.admin.authentication nsswitch,internal
options security.admin.nsswitchgroup <nisgrp0,nisgrp1:power>
```

This entry defines the groups within the NIS database that have permissions and roles for administration within Data ONTAP. In this case the group nisgrp0 will be mapped to the admin role, and the group nisgrp1 will be mapped to the power role.

Note: For further information on the configuration of the NIS service, refer to the “Data ONTAP 8.1.1 7-Mode File System and Protocol Administrators Guide.”

9 AutoSupport

AutoSupport provides a “call home” capability that can provide many benefits for the storage administrator. AutoSupport integrates event notification with automated support case creation so that significant issues with your storage controller can be immediately diagnosed by NetApp Support personnel or replacements automatically sent for failed drives. The My AutoSupport portal, which is an application hosted on the NetApp Support site at support.netapp.com, is a Web-based application that works in conjunction with AutoSupport to provide customers with information and tools designed to analyze, model, and optimize their storage infrastructure. My AutoSupport improves self-service support and the operational efficiency of your NetApp systems.

The default setting for the information that is sent to NetApp includes all message logs and other configuration data. NetApp recommends a close review of this information prior to placing the storage controller into production. The content has two settings for the periodic (daily or weekly) and triggered messages sent to NetApp: `complete` and `minimal`. The minimal setting will reduce the information that is sent to NetApp and sanitize other information that is sent. Using minimal mode increases case resolution times and requires some extra effort on your part to provide logs or other diagnostic data, if needed, to NetApp Support. It also reduces the number of features available to customers and partners via the My AutoSupport portal.

There are three methods to send AutoSupport information to NetApp: HTTPS (the default on new installations of Data ONTAP 8.1.x operating in 7-Mode), HTTP, and SMTP. The HTTPS transport should be used since HTTP and SMTP are clear text messages.

Best Practice

- Use the default transport (https) **`options autosupport.support.transport https.`**
- Review the content of the AutoSupport messages sent to NetApp. See the Support site kb article 1013073: “How to manually send AutoSupport to NetApp.”
- If it is determined that a minimal-content AutoSupport message is required by your security policy, enable only minimal-content AutoSupport messages: **`options autosupport.content minimal.`**

Information concerning the benefits of AutoSupport can be found in the AutoSupport portion of the NetApp Web site.

The “Monitoring the storage system” section of the “Data ONTAP 8.1.1 System Administration Guide for 7-Mode” provides information on the configuration of the AutoSupport service.

10 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 System Manager or another SDK ONTAPI® application, 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 was changed in the configuration files

For commands executed through the console, a telnet shell, or 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 HTTP(s).

For detailed information on audit logging and its capabilities, please refer to the “Audit logging” section of the “Data ONTAP 8.1.1 7-Mode System Administration Guide.”

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 syslog.conf for details.

11 Firewalling and Protocol Access Controls

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

Note: Refer to the “Data ONTAP 8.1.1 7-Mode Network Management Guide” for detailed information.

11.1 Protocol Blocking (Firewalling)

Data ONTAP provides a firewall for protocols (cifs, nfs, ftp, ndmp, iscsi, snapmirror). Protocol blocking can be seen as a protocol firewall. Some examples for protocol blocking are:

```
cli> options interface.blocked.cifs e5b

cli> options interface.blocked.nfs e1a,e1b

cli> options interface.blocked.iscsi e5b

cli> options interface.blocked.ftpd e5b,e1a,e1b

cli> options interface.blocked.snapmirror e4a,e4b

cli> options interface.blocked.cifs ""

cli> options interface.blocked.mgmt_data_traffic on (applies to e0M)
```

11.2 Protocol Access Filters

There are protocol access 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. The IP information can be either in IPv4 or IPv6 format. Each application then uses the filter on the listening socket to control access. Some examples are:

`cli> options ssh.access host=10.10.1.0/24` (allow network 10.10.1.0)

`cli> options telnet.access host=3FFE:81D0:107:2082::1/64` (allow host with prefix 3FFE:81D0:107:2082::1) `cli> options rsh.access host=-` (deny RSH)

`cli> options snapvault.access all` (allow all SnapVault connections)

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.

12 Vulnerability Scanners and Reporting

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.

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

12.1 Reporting Suspected Vulnerabilities

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 support cases, except that you should ask for the case to be escalated to the Vulnerability Response team.

Please refer to the NetApp Support site (Suspected Security Vulnerabilities) for further information.

Appendixes

Log-on Banners

The /etc/motd file is not present on the storage system by default. This also provides a post-login message to the cli authentication process.

Once created, the /etc/issue file provides a prelogin 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 8.1.1 7-Mode System Administration Guide.”

Best Practice
Create and maintain the /etc/issue and the /etc/motd files on your storage systems.

Maximums

The table below lists the maximums for Data ONTAP 8.1.1 7-Mode.

Table 12) Data ONTAP maximums.

Object	Maximum	Notes
Local User Accounts	96	

Object	Maximum	Notes
Password Length	256 characters	
Password Age	4,294,967,295 days	
Password Bad Login Lockout	4,294,967,295 attempts	
Interactive SSH Sessions per vFiler® Unit	1 session	
Noninteractive SSH Sessions	24 per system	
Concurrent HTTP Admin Connections	1,023	Connections using the login-http-admin capability
Concurrent Telnet Sessions	1 per system	
Concurrent FTP Connections	5,000 connections	
Concurrent RSH Sessions	24 per system / 4 per vFiler unit	
RLM System Event Log (SEL) Entries	4,000	Rolling FIFO list of events
SP System Event Log (SEL) Entries	4,000	Rolling FIFO list of events
BMC System Event Log (SEL) Entries	512	Rolling FIFO list of events
System Audit Log Entry	511 characters	This includes the entire entry, which includes the date time stamp, storage controller name, and so on
System Audit Logs	6 logs	They are numbered 0–5 auditlog.0, auditlog.1, and so on
System Audit Log Size	16 terabytes	The default is 10 megabytes
CIFS Audit Log Size	64 gigabytes	

Object	Maximum	Notes
CIFS Audit Logs (saved)	999 .evt files if configured	The default is no limit; it can be set to a value of 0 (no limit) to a value of 999
FTP Command Log Size	4 gigabytes	
FTP Transfer Log Size	4 gigabytes	
HTTP Log Size	4 gigabytes	
FTP Logs	100 logs	
HTTP Logs	100 logs	

Data ONTAP Log Locations

Table 13) 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

CIFS Protocol

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

CIFS Guidance Documents

TR-3771—“NetApp Storage Systems in a Microsoft Windows Environment”

TR-3457—“Unified Windows and UNIX Authentication Using Microsoft Active Directory Kerberos”

TR-3490—“NetApp Storage System Multiprotocol User Guide”

TR-3458—“Unified Windows and UNIX Authorization Using Microsoft Active Directory LDAP as a Directory Store”

TR-3595—“Auditing Quick Start Guide”

TR-3596—“Storage-Level Access Guard Quick Start Guide”

TR-3597—“Bulk Security Quick Start Guide”

Best Practice

- Set SMB signing On: options cifs.signing.enable on

Note: If you are using SMB1 this will cause an impact on the communications. Using SMB2 may reduce the impact of SMB signing.

- Set session authentication level to Kerberos only: options cifs.LMCompatibilityLevel 5
- Remove 'everyone/fullcontrol' from default shares: options cifs access <sharename> [-g] <user|group> <rights>
- Enable ABE on CIFS shares: cifs access <sharename> <–accessbasedenum>
- Set restrict anonymous: options cifs.restrict_anonymous 2
- Enable GPO support: options cifs.gpo.enable on
- Enable weekly changes of the machine password: options cifs.weekly_W2K_password_change on
- Disable NetBIOS over TCP: options cifs.netbios_over_tcp.enable off
- Enable CIFS audit: options cifs.audit.enable on
- Enable Data ONTAP account management audit: options cifs.audit.account_mgmt_events.enable on
- Enable the auditing of CIFS file access events: options cifs.audit.file_access_events.enable on
- Audit CIFS logons and logoffs: options cifs.audit.logon_events.enable on
- Familiarize yourself with the `fsecurity` command (see man pages volume 1: na_fsecurity)

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

- Avoid security access control lists (SACLs) that contain "Full Control" for "Everyone."
- Minimize the number of entries in the SACL for an object.
- To maximize the effectiveness of auditing, audit only the actions that are really interesting.
- Set an appropriate size for the event log file.

NFS Protocol

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

Best Practices

- Kerberos authentication—Enable Kerberos authentication on the export when the export is created. Refer to TR-3481 and the "File Access and Protocols Management Guide" for further information.
- LDAP signing and sealing with SASL and LDAP transport over SSL—Enable LDAP user lookup for authorization. Enable LDAP over SSL or SASL. Refer to NetApp technical report TR-3464 for information on setting up LDAP with NetApp storage systems.
- Enable NFSv4—Use NFSv4 because this enhances the ACL control of the file access.
- Disable NFSv2 and NFSv3 (assuming the clients can cope with NFSv4 only).
- Enable NFS over TCP—Use TCP as the transport for NFS sessions.
- Restrict the ability to mount to root-level accounts only (in the exports file).
- Restrict NFS mounts to low-numbered ports.
- Disable automatic export of volumes (`options nfs.export.auto-update off).`
- Disable provisional access for exports (`options nfs.export.allow_provisional_access off).`

NFS Guidance Documents

For further information on NFS refer to the following documents.

TR-3457—"Unified Windows and UNIX Authentication Using Microsoft Active Directory Kerberos"

TR-3464—"Integration of a NetApp Storage System with a UNIX-Based LDAP Server"

TR-3481—"Kerberized NFS in a NetApp Storage System Using a UNIX-Based Kerberos Authentication Server"

TR-3580—"NFSv4 Enhancements and Best Practices Guide: Data ONTAP Implementation"

"File Access and Protocols Management Guide"

Secure File Transfer Protocol

The Secure File Transfer Protocol (SFTP) is a secure replacement for the File Transfer Protocol (FTP). SFTP is based on the Secure Shell protocol.

Similar to FTP, SFTP is an interactive file transfer program that performs all operations over an encrypted SSH transport. Unlike FTP, SFTP encrypts both commands and data, providing effective protection against common network security risks. The SSH client and server provide both command-line SFTP tools and a graphical user interface for Windows users. SFTP encrypts the session, preventing the casual detection of your user name, password, or anything you have transmitted. This protocol assumes that it runs over a secure channel, that the server has already authenticated the user at the client end, and that the identity of the client user is externally available to the server implementation. SFTP runs from the SSH Connection Protocol as a subsystem.

Data ONTAP implements SFTP in accordance with version 03 of the Internet-Draft of the SSH File Transfer Protocol, which is available at http://tools.ietf.org/html/draft-ietf-secsh-filexfer-03.

Note: Refer to the "Data ONTAP 8.1.1 7-Mode File Access and Protocols Management Guide."

MultiStore

MultiStore® software is a feature of Data ONTAP software that enables you to partition the resources of a single storage system so that it appears as multiple vFiler unit storage systems on your network.

Each storage system created as a result of the partitioning is called a vFiler unit. A vFiler unit, using the resources assigned, delivers file access and block access services to its clients the same way that a storage system does.

The storage system on which you create vFiler units is called the hosting storage system. The storage and network resources used by the vFiler units exist on the hosting storage system. Each vFiler unit can be configured and administered independently from the hosting storage system and from other vFiler units, although some functions are reserved only for the hosting administrator.

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. You can add storage and network resources to a vFiler unit at any time. You can also remove these resources from a vFiler unit at any time.

You can manage MultiStore from the hosting storage system by using the command line or System Manager. You can perform tasks such as creating, starting or stopping, and destroying vFiler units. You can also manage resources and protocols and monitor the status of vFiler units.

Starting with Data ONTAP 8.1, as a vFiler unit administrator you can log in to a vFiler unit from an appropriate Secure Shell client application, such as PuTTY for Windows hosts or OpenSSH for UNIX hosts. You can execute commands directly on a vFiler unit through an interactive SSH session.

Note: Refer to the “Data ONTAP 8.1.1 7-Mode MultiStore Management Guide” for further details.

References / Links

- Cloud Control Matrix (CCM) by Cloud Security Alliance: https://cloudsecurityalliance.org/research/ccm/
- NetApp Support Site Statement of Volatility: http://support.netapp.com/NOW/products/volatility/

Version History

Version	Date	Document Version History
Version 1.0	September 2011	First issue for Data ONTAP 8.1RC1
Version 1.1	August 2012	Updated for Data ONTAP 8.1.1

Refer to the Interoperability Matrix Tool (IMT) on the NetApp Support site to validate that the exact product and feature versions described in this document are supported for your specific environment. The NetApp IMT defines the product components and versions that can be used to construct configurations that are supported by NetApp. Specific results depend on each customer's installation in accordance with published specifications.

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.

Go further, faster®

NetApp®

www.netapp.com