Technical Report

RBAC for Local Administration with Data ONTAP Operating in 7-Mode

Ron Demery CISSP, NetApp
March 2012 | TR-4062

Data ONTAP 8.1

This paper focuses on NetApp® Data ONTAP® 8.1 operating in 7-Mode. It explores the use of the default Data ONTAP roles and their capabilities. This paper is to be used as a companion to the Data ONTAP 8.1 7-Mode System Administration Guide.

TABLE OF CONTENTS

LIST OF TABLES

1 What Are Role-Based Access Controls?

Role-based access control (RBAC) is a method for managing the set of actions that a user or administrator can perform in a computing environment.

Historically, older computer operating systems allowed any user who had access to the system to perform any function. In fact, many systems did not distinguish between users at all. Most current operating systems offer, at a minimum, the ability to create several different users, each with a separate username and password. Once they were able to distinguish between users, operating systems began to employ user identification as a means to control access to files, directories, and other system objects. Examples of this are the file permissions used on UNIX® systems (and the NFS protocol) and the access control lists used on Windows® systems (and the CIFS protocol).

In addition to file access, there are other actions that should be managed for security reasons. For example, only the system administrator should be allowed to add new user accounts to the system. From this it is clear that the users who access a system fall into at least two categories, or roles: administrators and nonadministrators.

Although reserving certain functions for administrator-only access is a good start, additional problems need to be solved. Most organizations have multiple system administrators, some of whom require more privileges than others. By selectively granting or revoking privileges for each user, you can customize the degree of access that an administrator has to the system. For example, Microsoft® Windows offers this capability. The problem with this approach is that as the number of system administrators grows, it becomes difficult and time consuming to manage the set of capabilities granted to each administrator.

Role-based access controls solve this management problem by allowing you to define sets of capabilities (roles) that are not assigned to any particular user. Users are assigned to groups based on their job functions, and each group is granted the set of roles required to perform those functions. Using this method, the only configuration required for an individual administrator is to make sure that the administrator is a member of the appropriate groups; the administrator inherits all the correct capabilities because of the group membership and the roles assigned to those groups.

2 How Does RBAC Work in Data ONTAP?

Although the concept of role-based access controls is applicable to a wide range of operating systems and applications, the details of how RBAC is implemented vary depending on the OS or application in use. This section describes the terminology and architecture used in Data ONTAP. It is important to understand these concepts and definitions before configuring RBAC in Data ONTAP, especially if you have experience with RBAC implementations in other software, because the terminology or architecture differs among implementations.

The strategy to follow in Data ONTAP operating in 7-Mode is A → G → R → C. Accounts are assigned to groups, groups are assigned roles, and roles are assigned capabilities.

Best Practices
Create an account for each individual rather than allowing more than one person to access the same account.
Assign accounts the least privilege (capabilities) required to perform the task assigned.
Once new accounts are assigned, disable the root account.

2.1 Users, Entities, and Accounts

There are two types of accounts that interact with the administrative path of Data ONTAP: local accounts and domain user accounts.

A *local account* is an account that is authenticated in Data ONTAP.

A *domain user account* is a nonlocal user who belongs to a Windows domain and is authenticated by the domain.

Both local and domain user accounts, as discussed in this document, are assumed to be authorized system administrators. This document does not discuss nonadministrative users who access files on the system by using CIFS or NFS, or who use client systems that mount LUNs by using FCP or iSCSI. They have no ability to log into or manage a Data ONTAP system unless they have been specifically defined as either users or domain users with the `useradmin` command.

For more information, refer to "How to Manage Users" in the Data ONTAP 8.1 7-Mode System Administration Guide.

2.2 Groups

A *group* is a collection of local and/or domain user accounts. Groups can be assigned one or more roles.

Note: Groups defined in Data ONTAP are separate from groups defined in other contexts, such as a Microsoft Active Directory® server. This is true even if the groups in Data ONTAP have the same names as groups elsewhere in your environment.

When you create new local and/or domain user accounts, Data ONTAP requires group membership to be specified. Therefore it's best to create appropriate groups before defining users or domain users.

The default groups are administrators, backup operators, compliance administrators, guests, power users, and users.

For more information, refer to "How to Manage Groups" in the Data ONTAP 8.1 7-Mode System Administration Guide.

Table 1) Data ONTAP 8.1 operating in 7-Mode default groups.

Name	Description	Role
Administrators	Fully administer the system	admin
Backup operators	Special file permission to back up files	backup, none
Compliance administrators	Compliance (NetApp SnapLock®) operations	compliance
Guest	Guest access	none
Power users	Entry-level administrators	power
Users	Local users	audit

2.3 Roles

A *role* is defined as a named set of capabilities. Data ONTAP comes with several roles predefined, and users can create additional roles or modify the roles provided.

The default roles are admin, audit, backup, compliance, none, power, and root.

For more information, refer to "How to Manage Roles" in the Data ONTAP 8.1 7-Mode System Administration Guide.

Table 2) Data ONTAP 8.1 operating in 7-Mode default roles.

Name	Capabilities
admin	login-*, cli-*, api-*, security-*
audit	api-snmp-get, api-snmp-get-next
backup	login-ndmp
compliance	cli-cifs*, cli-exportfs*, cli-nfs*, cli-useradmin*, api-cifs-*, api-nfs-*, login-telnet, login-http-admin, login-rsh, login-ssh, api-system-api-*, cli-snaplock*, api-snaplock-*, api-file-*, compliance-*
none	None
power	cli-cifs*, cli-exportfs*, cli-nfs*, cli-useradmin*, api-cifs-*, api-nfs-*, login-telnet, login-http-admin, login-rsh, login-ssh
root	All

2.4 Capabilities

Data ONTAP supports the following capability types: login, cli, security, api, and compliance.

Table 3) Data ONTAP 8.1 operating in 7-Mode supported capabilities.

Capability	Description
login	Grants the specified role login capabilities. **`login-*`** grants the specified role the capability to log in through all supported protocols. **`login- <protocol>`** grants the specified role the capability to log in through a specified protocol. The following protocols are supported: • **`login-console`** grants the specified role the capability to log in to the storage system by using the console. • **`login-http-admin`** grants the specified role the capability to log in to the storage system by using HTTP. • **`login-ndmp`** grants the specified role the capability to make NDMP requests. • **`login-rsh`** grants the specified role the capability to log in to the storage system by using RSH. • **`login-snmp`** grants the specified role the capability to log in to the storage system by using SNMPv3. • **`login-sp`** grants the specified role the capability to log in to the SP or the RLM by using SSH. • **`login-ssh`** grants the specified role the capability to log in to the storage system by using SSH. • **`login-telnet`** grants the specified role the capability to log in to the storage system by using Telnet.

Capability	Description
cli	Grants the specified role the capability to execute one or more Data ONTAP command line interface (CLI) commands. **cli-*** grants the specified role the capability to execute all supported CLI commands. **cli- cmd*** grants the specified role the capability to execute all commands associated with the CLI command **cmd**. For example, the following command grants the specified role the capability to execute all **vol** commands: **useradmin role modify status_gatherer -a cli-vol*** Users with **cli** capability also require at least one login capability to execute CLI commands.
security	Grants the specified role security-related capabilities, such as the capability to change other users' passwords or to invoke the CLI **priv set advanced** command. **security-*** grants the specified role all security capabilities. **security- <capability>** grants the specified role one of the following security capabilities: • **security-api-vfiler** grants the specified role the capability to forward or tunnel Data ONTAP APIs from the physical storage system into a vFiler® unit for execution. • **security-passwd-change-others** grants the specified role the capability to change the passwords of all users with equal or fewer capabilities. • **security-priv-advanced** grants the specified role the capability to access the advanced CLI commands. • **security-load-lclgroups** grants the specified role the capability to reload the **lclgroups.cfg** file. • **security-complete-user-control** grants the specified role the capability to create, modify, and delete users, groups, and roles with greater capabilities.
api	Grants the specified role the capability to execute Data ONTAP API calls. **api-*** grants the specified role all API capabilities. **api-<api_call_family-*>** grants the specified role the capability to call all API routines in the family **api_call_family**. **api-<api_call>** grants the specified role the capability to call the API routine **api_call**. **Note:** You have more fine-grained control of the command set with the API capabilities because you can give subcommand capabilities as well. Users with API capability also require the **login-http-admin** capability to execute API calls.

Capability	Description
compliance	Grants the specified role the capability to execute compliance-related operations. **`compliance-*`** grants the specified role the capability to execute all compliance-related operations. **`compliance-privileged-delete`** grants the specified role the capability to execute privileged deletion of compliance data. **Note:** The compliance capabilities (**`compliance-*`**) are included in the default capabilities of the compliance role. The compliance capabilities cannot be removed from the compliance role or added to other roles.

3 Integration With Microsoft Active Directory

The ability to define domain users that are authenticated by an Active Directory 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 (username, 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

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

```
OntapSC> useradmin domainuser delete domain\"Domain Admins" -g administrators
```

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
```

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.

4 Custom Role for the RLM or SP Only Account

You can manage a storage system remotely by using a remote management device, which can be the service processor (SP) or the Remote LAN Module (RLM). The remote management device stays operational regardless of the operating state of the system. It provides remote platform management capabilities, including remote access, monitoring, troubleshooting, logging, and alerting features.

Local accounts are required for authentication to the RLM and SP. The accounts that can authenticate to the RLM and SP must have **`login-sp`** capability. The management of the hardware may sometimes be a separate IT role from the management of Data ONTAP. To meet those requirements, you can:

1. Create a role with the **`login-sp`** capability.
2. Create a group with the role created in step 1.
3. Create a local account and assign it only to the group created in step 2.

```
OntapSC> useradmin role add sp-only -a login-sp
Role <sp-only> added.

OntapSC> useradmin group add hardware-admins -c sp-only
Group <hardware-admins> added.

OntapSC> useradmin user add hwtech -g hardware-admins
New password:
Retype new password:
User <hwtech> added.
```

The account **`hwtech`** cannot authenticate into Data ONTAP through the use of the **`system console`** command at the RLM or SP prompt. When the user attempts to authenticate, an error message appears stating that the user does not have the `login-console` capability.

For more information about the remote management capabilities of the SP and RLM, see "Managing a storage system remotely" in the Data ONTAP 8.1 7-Mode System Administrators Guide.

Appendix

This appendix describes the CLI capabilities and the top-level API capabilities.

Command Line Interface (CLI) Capabilities

There may be times when you want to build a custom role for a task that is specific to a junior administrator. Suppose that you need to provide ssh access to an administrator and the only task that person will have is to manage aggregates and volumes.

The first steps are to add a role with the capability to log in using ssh, add that role to a new group, and add a user to that group. Then attempt to perform the commands that the new user account will use to perform the assigned task. If the account does not possess the capabilities required to perform a function, the Data ONTAP console displays an error message.

```
OntapSC> useradmin role add ssh-admin -a login-ssh
Role <ssh-admin> added.
OntapSC> useradmin group add ssh-only -r ssh-admin
Group <ssh-only> added.
OntapSC> useradmin user add StgAdmin -g ssh-only
New password:
Retype new password:
User <StgAdmin> added.
```

When the new user has been added, you can test to see the error messages that the Data ONTAP console displays.

```
login as: stgadmin
stgadmin@x.x.x.x's password:

OntapSC> version
Permission denied, user stgadmin does not have access to version
OntapSC> Mon Mar 19 11:26:12 EST [OntapSC:useradmin.unauthorized.user:warning]: User 'stgadmin'
denied access - missing required capability: 'cli-version'

OntapSC> aggr
Permission denied, user stgadmin does not have access to aggr
OntapSC> Mon Mar 19 11:26:22 EST [OntapSC:useradmin.unauthorized.user:warning]: User 'stgadmin'
denied access - missing required capability: 'cli-aggr'

OntapSC> df
Permission denied, user stgadmin does not have access to df
OntapSC> Mon Mar 19 11:26:29 EST [OntapSC:useradmin.unauthorized.user:warning]: User 'stgadmin'
denied access - missing required capability: 'cli-df'

OntapSC> vol status
Permission denied, user stgadmin does not have access to vol
OntapSC> Mon Mar 19 11:26:41 EST [OntapSC:useradmin.unauthorized.user:warning]: User 'stgadmin'
denied access - missing required capability: 'cli-vol'

OntapSC> useradmin user modify stgadmin -g administrators
Permission denied, user stgadmin does not have access to useradmin
OntapSC> Mon Mar 19 11:27:19 EST [OntapSC:useradmin.unauthorized.user:warning]: User 'stgadmin'
denied access - missing required capability: 'cli-useradmin'
```

The account can log in over ssh but has no other capabilities. Because you want the user to have only the ability to create aggregates, manage volumes, and list the space used by the volumes, you need to add cli-aggr, cli-vol, and cli-df to the role that is assigned to the group of which this user is a member (ssh-admin).

Log in as an admin role user:

```
OntapSC> useradmin role modify ssh-admin -a login-ssh,cli-df,cli-aggr,cli-vol
Role <ssh-admin> modified.
```

```
OntapSC>
OntapSC> useradmin role list ssh-admin
Name:    ssh-admin
Info:    Storage Provisioning Admin
Allowed Capabilities: login-ssh,cli-df,cli-aggr,cli-vol
```

Now log into the storage system via ssh with the stgadmin account and see which commands you can execute:

```
login as: stgadmin
stgadmin@x.x.x.x's password:

OntapSC> version
Permission denied, user stgadmin does not have access to version
OntapSC> Mon Mar 19 12:32:07 EST [OntapSC:useradmin.unauthorized.user:warning]: User 'stgadmin'
denied access - missing required capability: 'cli-version'


OntapSC> df
Filesystem              kbytes       used      avail capacity  Mounted on
/vol/vol0/              828324     333288     495036      40%  /vol/vol0/
/vol/vol0/.snapshot      43592     113480          0     260%  /vol/vol0/.snapshot

OntapSC> vol status
         Volume State           Status            Options
           vol0 online          raid_dp, flex     root
                                64-bit
OntapSC> aggr
The following commands are available; for more information
type "aggr help <command>"
add                 mirror              rename              split
copy                offline             restrict            status
create              online              scrub               undestroy
destroy             options             show_space          verify
media_scrub
OntapSC> aggr status
           Aggr State           Status            Options
          aggr0 online          raid_dp, aggr     root
                                64-bit
OntapSC> exportfs
Permission denied, user stgadmin does not have access to exportfs
OntapSC> Mon Mar 19 12:33:58 EST [OntapSC:useradmin.unauthorized.user:warning]: User 'stgadmin'
denied access - missing required capability: 'cli-exportfs'
```

As a result of this testing, you find that if you want the stgadmin account to be able to create NFS exports, you must also give that role the cli-exportfs capability.

It is possible to assign multiple roles to a single group. As a test, create a role (nfs-export) with the capability cli-exportfs and add it to the ssh-only group.

Log in as an admin role user:

```
OntapSC> useradmin role add nfs-export -a cli-exportfs
Role <nfs-export> added.
OntapSC> Mon Mar 19 12:43:52 EST [OntapSC:useradmin.added.deleted:info]: The role 'nfs-export'
has been added.


OntapSC> useradmin group modify ssh-only -r ssh-admin,nfs-export
Group <ssh-only> modified.
OntapSC> Mon Mar 19 12:45:53 EST [OntapSC:useradmin.added.deleted:info]: The group 'ssh-only' has
been modified.


OntapSC> useradmin group list ssh-only
Name: ssh-only
Info:
Rid: 131077
```

```
Roles: ssh-admin,nfs-export
Allowed Capabilities: login-ssh,cli-df,cli-aggr,cli-vol,cli-exportfs
```

Now test to make sure that the stgadmin account can perform the `exportfs` command.

```
login as: stgadmin
stgadmin@x.x.x.x's password:

smte-rc1-7m-01> exportfs
/vol/vol0/home -sec=sys,rw,nosuid
/vol/vol0      -sec=sys,rw,anon=0,nosuid
```

Also notice that the cli-x capabilities are only at the first-level commands. When using the cli capabilities, it is not possible to create a role that can, for example, only view the status of a volume and not create, destroy, or otherwise modify the volume. If you want to have more granular control by using the Data ONTAP RBAC, it is necessary to use the API capabilities and to use System Manager or Windows PowerShell™, or to develop a custom SDK application that uses the login-http-admin method.

Table 4 lists the top-level capabilities that are available in Data ONTAP 8.1 operating in 7-Mode. This list of capabilities is derived from Data ONTAP 8.1 Commands: Manual Page Reference, Volume 1.

Table 4) cli capabilities and description.

CLI Command	Description
acpadmin	Commands for managing alternate control path administration.
aggr	Commands for managing aggregates, displaying aggregate status, and copying aggregates
arp	Display and control address resolution
autosupport	Manage and view the AutoSupport™ notification daemon
backup	Manage backups
bmc	Commands for use with a baseboard management controller (BMC)
cdpd	View the neighbors of the storage controller that are discovered by using Cisco® Discovery Protocol (CDP) v1 and associated statistics
cf	Control the takeover and giveback operations of the systems in a cluster **charmap** command for managing per-volume character maps
charmap	Command for managing per-volume character maps
cifs	Summary of CIFS commands
clone	Manage file and subfile cloning
config	Command for configuration management
date	Display or set date and time
dcb	Manage Data Center Bridging (DCB) configuration for DCB-capable interfaces
df	Display free disk space
disk	RAID disk configuration control commands

CLI Command	Description
disk_fw_update	Update disk firmware
dns	Display DNS information and control DNS subsystem
download	Install new version of Data ONTAP
du	Display the number of blocks that are used in a file
dump	File system backup
echo	Display command line arguments
ems	Invoke commands to the Data ONTAP Event Management System (EMS)
environment	Display information about the system's physical environment
exportfs	Export or unexport a file system path, making it available or unavailable, respectively, for mounting by NFS clients
fcadmin	Commands for managing Fibre Channel adapters
fcnic	Command to control out-of-order (OOD) frame delivery on Fibre Channel Virtual Interface (FCVI) NIC adapters
fcp	Commands for managing Fibre Channel target adapters and the FCP target protocol
fcstat	Fibre Channel statistics functions
file	Manage individual files
flexcache	Commands for administering NetApp FlexCache® volumes
fsecurity	Summary of **fsecurity** commands
ftp	Display FTP statistics
halt	Stop the storage controller
help	Print a summary of commands and help strings
hostname	Set or display the storage controller name
httpstat	Display HTTP statistics
ic	Monitor the HA interconnect
ifconfig	Configure network interface parameters
ifgrp	Manage interface group (ifgrp) configuration
ifstat	Display device-level statistics for network interfaces
igroup	Commands for managing initiator groups

CLI Command	Description
ipsec	Manipulate the IPsec SP, SA, and certificate databases and display IPsec statistics
ipspace	ipspace operations
iscsi	Manage iSCSI service
key_manager	External key server management commands
keymgr	Key and certificate management
license	License Data ONTAP services
lock	Manage lock records
logger	Record message in system logs
logout	Terminate a telnet session
lun	Commands for managing LUNs
man	Locate and display reference manual pages
maxfiles	Increase the number of files the volume can hold
mt	Manage magnetic tape positioning and control
nbtstat	Display information about the NetBIOS over TCP connection
ndmpcopy	Transfer directory trees between systems by using NDMP
ndmpd	Manage NDMP service
ndp	Control and diagnose IPv6 neighbor discovery protocol
netdiag	Perform network diagnostics
netstat	Show network status
nfs	Manage Network File System service
nfsstat	Display NFS statistics
options	Display or set system options
orouted	Old network routing daemon
partner	Access the data on the partner in takeover mode
passwd	Modify the system administrative user's password data
ping	Send ICMP ECHO_REQUEST packets to network hosts
ping6	Send ICMPv6 ECHO_REQUEST packets to network hosts

CLI Command	Description
pktt	Control on-controller packet tracing
portset	Commands for managing portsets
priority	Commands for managing priority resources
priv	Control per-connection privilege settings
qtree	Create and manage qtrees
quota	Control system disk quotas
radius	Manage RADIUS client protocol and components
rdate	Set system date from a remote host
rdfile	Read a WAFL® (Write Anywhere File Layout) file
reallocate	Command for managing reallocation of files, LUNs, volumes, and aggregates
reboot	Stop and then restart the system
restore	File system restore
revert_to	Revert the file system to a previous release
rlm	Commands for use with a Remote LAN Module (RLM)
route	Manually manipulate the routing table
routed	Manage the network RIP and router discovery routing daemon
rshstat	Print the information about active rsh sessions
sasadmin	Commands for managing serial attached SCSI (SAS) adapters
sasstat	Commands for viewing the status of the serial attached SCSI (SAS) adapters
savecore	Save a core dump
sectrace	Manage permission tracing filters
secureadmin	Command for secure administration of the appliance
setup	Update system configuration
sftp	Display SFTP (SSH File Transfer Protocol) statistics
shelfchk	Verify the communication of environmental information between disk shelves and the node
sis	Advanced Single Instance Storage (SIS) management
smtape	Manage image-based backup and restore

CLI Command	Description
snap	Manage Snapshot™ copies
snaplock	Manage compliance-related operations
snapmirror	Manage volume and qtree mirroring
snapvault	Manage disk-based data protection
snmp	Set and query SNMP agent variables
software	Install or upgrade Data ONTAP
source	Read and execute a file of system commands
sp	Commands for use with a service processor (SP)
stats	Command for collecting and viewing statistical information
storage	Commands for managing the disks and SCSI and Fibre Channel adapters in the storage subsystem
sysconfig	Display system configuration information
sysstat	Report system performance statistics
system	View system information
timezone	Set and obtain the local time zone
traceroute	Print the route that packets take to a network host
traceroute6	Print the route that IPv6 packets take to a network host
ups	Control the monitoring of UPS (uninterruptable power supply)
uptime	Show how long the system has been up
useradmin	Administer system access controls
version	Display Data ONTAP version
vfiler	Manage VFiler operations
vlan	Manage VLAN interface configuration
vmservices	Manage services for Data ONTAP running in a virtual machine
vol	Commands for managing volumes, displaying volume status, and copying volumes
vscan	Control virus scanning for files on the system
wcc	Manage WAFL credential cache
wrfile	Write a WAFL file

CLI Command	Description
ypcat	Print values from an NIS database
ypgroup	Display the group file entries cached locally from the NIS server if NIS is enabled
ypmatch	Print matching values from an NIS database
ypwhich	Display the NIS server if NIS is enabled

API Capabilities for NetApp Management SDK 4.1

This list is taken from the NetApp Manageability SDK 4.1 (NMSDK). For information about the NMSDK, refer to the NetApp Support site.

As stated in the previous section, it is not possible to restrict a role by using the cli capabilities only to view the status of a volume and not delete or offline the volume. Using the api capabilities makes this possible.

For example, to assign the ability for a user to only view the status of the volume and not give them any other functions, you would use the Manage ONTAP® SDK application.

NetApp recommendes using the HTTPS connection method when communicating to the storage controller. You need to set two settings on the storage controller. First, enable ssl and TLS; and second, make sure that `httpd.admin.enable` is off and `httpd.admin.ssl.enable` is on.

In reviewing the sample code included in the NetApp Manageability SDK in order to view the status of a volume, you may want to include the following volume capabilities:

- `api-volume-list-info*`

Note: In this case, the use of '*' is acceptable because it includes the other list (read only) functions that are needed to return a successful function call.

```
OntapSC> useradmin role add newrole -a login-http-admin,api-volume-list-info*
```

The Data ONTAP APIs are used to access and manage the NetApp storage system. This proprietary set of APIs includes APIs for security management, license management, backup and recovery, data replication, data archiving, and so on.

Table 5) API top-level capabilities for NMSDK 4.1.

Name	Description
aggr	Aggregate information and management
cf	Cluster-failover operations
cifs	CIFS configuration and management
clock	System time zone and date management
clone	Manage file and subfile cloning operation
consistency	Manage consistency groups
copyoffload	vStorage Copy Offload commands for storage array copy operations

Name	Description
diagnosis	Diagnosis Manage ONTAP SDK
disk	Disk-related operations
ems	Event Management System (EMS) APIs
fc	Fibre Channel adapter configuration
fcp	Fibre Channel protocol management
fcport	Fibre Channel port operations that manage Fibre Channel
file	Support file system operations
flash	Flash Management Module APIs
fpolicy	File policy management and configuration
ic	Storage Failover Interconnect APIs
igroup	Initiator group operations
ipspace	Manage ipspace
iscsi	Manage and monitor iSCSI
license	Manage license code
lock	Configure and manage Lock Manager
lun	Manage and monitor LUNs
nameservice	Obtain nameservice information
net	Access Data ONTAP network management
nfs	Configure and manage NFS in Data ONTAP
options	Manage option values
perf	Manage counters of various system performance objects
portset	Port set operations
priority	Manages priority scheduling operations
qtree	Manage qtrees
quota	Manage and edit quotas
radius	Access to Data ONTAP RADIUS client management (iSCSI Chap Authentication)
reallocate	Manage LUN and file optimization and reallocation operations
rsh	RSH information
ses	SCSI enclosure services-related operations
sis	Manage volume deduplication and compression
snaplock	SnapLock information and management

Name	Description
snapmirror	Manage SnapMirror®
snapshot	Manage Snapshot copies
snapvault	SnapVault® management APIs
snmp	Manage SNMP and retrieve MIB values
software	Software package information and management
storage-adapter	Storage adapter operations
storage-array	Commands to monitor and manipulate back-end storage arrays
storage-disk	Storage-disk-related operations
storage-initiator	Commands to monitor and view initiator port traffic
system	System information
useradmin	Configure and manage Useradmin
vfiler	Configure and manage vFiler
vmservices	Services for virtual machine platforms
volume	Volume information and management
wafl	Utility functions for agents

Version History

Version	Date	Document Version History
Version 1.0	March 2012	Initial Release