Role-Based Access Control for Clustered Data ONTAP

Jeff Asher, Steve Ryles, Hadrian Baron, Bryan Walsh, Mrinal Devadas

January 2015 | TR-4368

Version 1.0

Abstract

One of the most challenging problems in managing access to data within organizations is the complexity of security administration and user-profile management. Role-based access control has become the predominant model for advanced access control because it reduces the complexity and cost of administration.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1 Introduction

The NetApp® clustered Data ONTAP® operating system offers an exponential improvement to security management for users and groups managing hardware, software, and data on NetApp systems. This document furnishes the reader with a practical approach to understanding and implementing this new security model. This report focuses on clustered Data ONTAP 8.3.

Role-based access control (RBAC) is a method for managing the set of actions that a user or a group of users might perform in a computing environment. Within most computing environments, it is necessary to control access to data and other system objects so that only users with the appropriate permissions can view or alter them. In general, users who access a system fall into at least two categories, or roles: administrators and nonadministrators. For example, only the system administrator should be allowed to add new user accounts to the system.

Having two categories of users might not be sufficient. Organizations have multiple system administrators who require different privileges depending on the system resources they need to administer. You can control all access to system resources by selectively granting or revoking privileges to individual users and groups; however, it is difficult and time consuming to manage the set of capabilities granted to each administrator as the number of system administrators grows. RBAC solves this management problem. It is an approach to restricting system access to authorized users based on their job function and with it you can implement mandatory access control or discretionary access control.

2 How RBAC Works in Clustered Data ONTAP

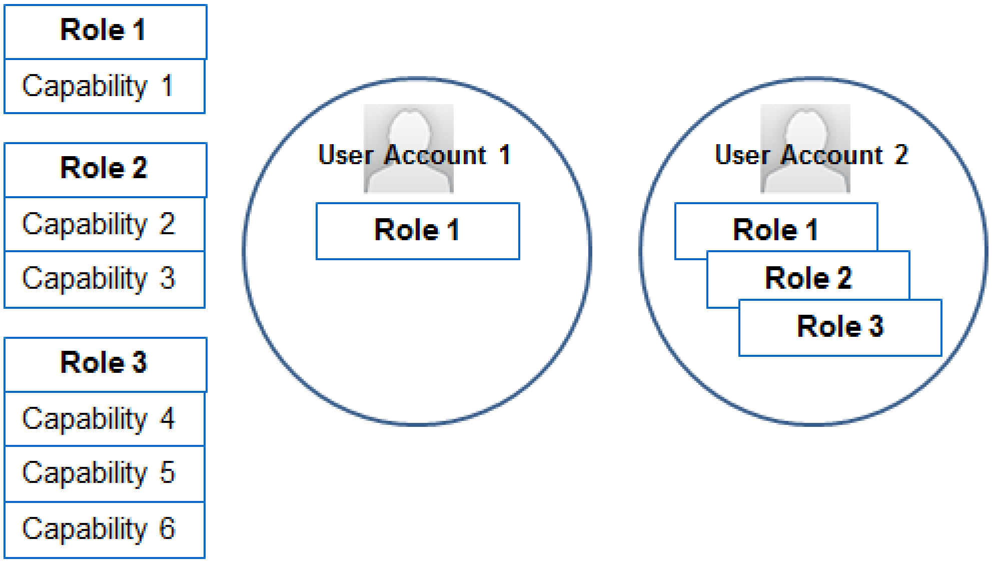
Although the overall concept of role-based access control is applicable to a wide range of operating systems and applications, the details of how RBAC is implemented vary depending on the operating system or application in use. This section describes the specific terminology and architecture used in clustered Data ONTAP. It is important that you understand these concepts and definitions because the terminology and architecture in clustered Data ONTAP might be different from implementations you used in the past.

The strategy to follow is: **A**ccounts are assigned **r**oles and **r**oles are assigned **c**apabilities (A.R.C.).

You define sets of capabilities that are assigned to any particular user. Users are assigned to roles based on their job functions and each role is granted the set of rules required to perform those functions. Using this method, the only configuration an individual administrator must make is to make sure that the user or group is a member of the appropriate roles. The administrator will then inherit all the correct capabilities because of the member's group membership and the roles assigned to those roles.

Refer to product documentation for Data ONTAP 8.3 for specific information on creating custom roles and assigning them to users and groups that belong to your Windows® Active Directory® domain.

Figure 1) Basic security model in role-based access control.



Also, see Figure 3, Example of creating custom roles using OnCommand System Manager.

2.1 Users and Accounts

A user is defined as an account that is authenticated on the NetApp system. A domain user is defined as a nonlocal user who belongs to a Windows domain and is authenticated by the domain. Both local users and domain users represent individual, authenticated humans. The user accounts discussed in this document are assumed to be administrative user accounts and not data access user accounts. Data access user account management is covered in the System Administration Guide for SVM Administrators.

Clustered Data ONTAP implements user accounts differently than Data ONTAP operating in 7-Mode. In clustered Data ONTAP, user accounts are created as either cluster accounts or storage virtual machine (SVM) accounts. Cluster user accounts can administer the cluster and all SVMs in that cluster. SVM user accounts are limited to executing commands that only show or affect objects in that SVM. A user logged in to an SVM user account only has access to that storage virtual machine.

User accounts must be created with a specified method to access the cluster or SVM. Table 1 lists the access methods and who can use them.

2.2 Roles

A role is defined as a named set of capabilities. Clustered Data ONTAP defines roles across a cluster and for individual SVMs. There are several predefined roles for each context and each role has a predefined set of capabilities. Each role can execute different sets of commands and has different access levels that can be used with those commands.

Table 1) Predefined roles for cluster users.

Role	Capability
admin	Has full administrative capabilities on the cluster and all SVMs in that cluster
autosupport	Allows users to generate and send NetApp AutoSupport™ messages and has no additional capabilities
backup	Permits only the commands required to configure NDMP and NDMP-related commands
readonly	Shows most settings and objects on the cluster, but the only change that a user with the *readonly* role can make is to his or her own password

The first role that an administrator becomes familiar with is the *admin* role. The default cluster administration user, *admin*, is assigned to the role *admin*.

Note that in some cases the user name and role name are identical, but this is not always the case. The user *admin* and role *admin* are different objects and should not be confused. Additional cluster administrator user accounts can be created, and you can also assign those accounts to the *admin* role.

There are also predefined roles that are scoped to individual SVMs that are present by default when the SVM is created. The *vsadmin* role allows a user almost full administrative control over an SVM and its objects. The commands that are restricted from the *vsadmin* role, such as *volume move*, affect the cluster or other SVMs, which can negatively affect the performance of the nodes serving that volume and by extension other SVMs.

Note: The `vsadmin` role cannot be used for direct SVM credentials in the Virtual Storage Console (VSC). This role is used mostly in multi-tenancy environments/infrastructures; however, it is not an access solution for every application in a given infrastructure. The VSC has specific privilege requirements that surpass what `vsadmin` privileges provide. For OffTap producs, it is highly recommended using the ONTAP RBAC User Creator tool to craft a role and user tailored not just to VSC, but to the particular operations that VSC is expected to perform. See *Section 8, RBAC User Creator*.

Other predefined roles for SVMs include the *vsadmin-volume* role, the *vsadmin-protocol* role, the *vsadmin-backup* role, and the *vsadmin-readonly* role. You can find additional information on all predefined roles in the "Managing Access to the Cluster" section of the System Administration Guide for Cluster Administrators.

Roles can also be created by a cluster administrator and privileges can be assigned to or restricted from those roles. Whether the role is applied to the cluster or an SVM, it can be created only by cluster administrator users whose roles have that capability. An administrator user for an SVM cannot create a role within that SVM.

2.3 Capabilities

The combination of a command and an access level is called a *capability*. It should be noted that the capabilities of the predefined roles cannot be changed.

A *command* is a specific instruction; however, when defining roles, a *command* can also be an entire command tree. For example, the `volume` command encompasses all commands available under that tree, while `volume snapshot policy show` is also a command.

The access levels available to be used with a command are *all*, *readonly*, and *none*. The *all* access level permits full access to all commands, while the *readonly* access level permits access only to the show commands under that command tree. The *none* access level does not permit the use of the specified command at all. In effect, that command does not exist for that role. If a user tries to execute a command that has an access level of *none* assigned to that user's role, an error message stating that the command is not recognized is returned.

2.4 Login Applications and Authentication Methods

In clustered Data ONTAP, to access the cluster or SVM you must link user accounts with an application. Cluster user accounts can use all methods, while SVM user accounts can use only HTTP, ONTAPI, SNMP, and SSH.

Table 2) Access methods for creating user account.

Access Method	Cluster User Account	SVM User Account
console	✓	
http (includes https)	✓	✓
ontapi	✓	✓

Access Method	Cluster User Account	SVM User Account
rsh (disabled by default)	✓	
service-processor	✓	
snmp	✓	✓
ssh	✓	✓
telnet (disabled by default)	✓	

When the user account is created, an authentication method must also be specified. A user account can have different authentication methods for each access method. Valid authentication methods are:

- SSL certificate
- SNMP community strings
- Windows Active Directory authentication
- LDAP or NIS authentication
- User password
- SSH public key authentication
- SNMP user-based security model

When you create a new user account with the authentication method of “password,” you must enter a password for the user. Any subsequent access methods that you configure for that user that use the password authentication method will use the user’s latest password.

3 Aligning Roles and Access Control with Microsoft Windows Active Directory Servers

In this section we will attempt to show similarities between the security model followed by Microsoft in Windows Server and clustered Data ONTAP.

In a single Active Directory (AD) domain environment, Microsoft's implementation of RBAC leverages different security group scopes:

- Global security groups: Domain security groups with global scope represent business roles or job functions within the domain. These groups might contain accounts and other global groups from the same domain, and they can be used by resources in any domain in the forest. They can be changed frequently without causing global catalog replication.
- Domain local security groups: Domain security groups with domain local scope describe the low-level permissions or user rights to which they are assigned. These groups can be used only by systems in the same domain. Domain local groups might may contain accounts, global groups, and universal groups from any domain, as well as domain local groups from the same domain.

Clustered Data ONTAP uses AGDLP[1] (account, global, domain local, permission). Security roles are defined for cluster and SVM users with the expectation that these roles will hardly ever change; however, membership of these roles will change as people move through the organization. Once a role is defined and access criteria specified, it is easy to manage the role.

Typically, once role access specifications are defined they are not changed; however, membership in a role can change to adapt to a user's responsibilities. The guiding principle is to keep administration at the role level to allow more efficient management of access control.

By default, clustered Data ONTAP 8.3 has 10 security roles: 5 roles apply to the cluster and 5 to the SVM. Microsoft® Windows 2012 Server has 14 default security groups. For details, see http://technet.microsoft.com/en-us/library/cc771990.aspx.

Table 3) Default roles in clustered Data ONTAP 8.3.

Role Name (Scope)	Explanation
admin (cluster)	Super user for the cluster
autosupport (cluster)	Allows customization and viewing of AutoSupport settings
backup (cluster)	Allows configuration of NDMP services and viewing user capabilities
none (cluster)	No access to commands on the clustershell
readonly (cluster)	Read-only access to all commands on the clustershell
vsadmin (SVM)	Super user for the SVM
vsadmin-backup (SVM)	Backup user with access to manipulate NDMP settings
vsadmin-protocol (SVM)	Admin user with access to manage user credentials, protocol configuration, and settings for the SVM
vsadmin-volume (SVM)	Similar capabilities as the `vsadmin-protocol` role but with additional privileges to manage name services of the SVM
vsadmin-readonly (SVM)	Ability to view all configuration information of the SVM

The default roles give us some indication of the security roles that can be defined on the cluster or an SVM. We can use the 14 default security groups in Microsoft Windows Active Directory on a Microsoft Windows 2012 Server (http://technet.microsoft.com/en-us/library/cc771990.aspx) as reference to define security roles in Data ONTAP to segregate user responsibilities.

Table 4 lists the default security groups available in Microsoft Windows Active Directory with a brief explanation of how the role could be interpreted in a clustered Data ONTAP deployment.

[1] AGDLP (an acronym for "account, global, domain local, permission") briefly summarizes Microsoft's recommendations for implementing role-based access control (RBAC) using nested groups in a native-mode Active Directory (AD) domain: User and computer accounts are members of global groups that represent business roles, which are members of domain local groups that describe resource permissions or user rights assignments. Retrieved November 22, 2014, from Wikipedia, the free encyclopedia http://en.wikipedia.org/wiki/AGDLP.

Since Microsoft Windows servers have a different set of capabilities than Data ONTAP, not all the roles have an equivalent. The security roles listed below are in addition to the default roles described in the previous table.

Table 4) Map of default security groups in Windows 2012 servers to roles in clustered Data ONTAP.

Windows Security Group	Possible Equivalent Security Role in Data ONTAP
Administrators	Similar to the *admin* and *vsadmin* roles. The role can be defined for cluster and SVM users. Ability to create new aggregates and remove nodes from the cluster. The role can be defined for cluster users. Ability to create new aggregates and remove nodes from the cluster. The role can be defined for cluster users.
Backup Operators	Some of the capability is covered by the cluster level role of backup and some by the SVM-level *vsadmin-backup* role. A new security role can be created to allow the user to create cluster and SVM peer relations, set up and initialize NetApp SnapMirror® and SnapVault® relations, define retention policies, manage NDMP configuration, and perform restore operations. The role can be defined for cluster and SVM users.
Cryptographic Operators	Ability to manage SSL certificates for SVMs. The role can be defined for SVM users. Ability to manage the Kerberos configuration of the SVM. The role can be defined for cluster users. Ability to lock and unlock cluster and SVM admins. The role can be defined for cluster and SVM users.
Guests	
Users	
Power Users	Ability to create and manage policies for Quality of Service (QoS), SnapMirror, SnapVault, and NetApp Snapshot® copies. The role can be defined for SVM users. Ability to add or remove user accounts to defined security roles. This role does not create security roles. The role can be defined for cluster and SVM users. Ability to create and delete SVMs. The role can be defined for cluster users.
Network Configuration Operators	Ability to manage LIF attributes of the cluster and SVM. This includes creation, modification, and deletion of LIFs that belong to the cluster and SVM. The role can be defined for cluster users.
Performance Log Users	
Performance Monitor Users	Ability to create and modify QoS policies used by an SVM. There is some overlap of this role with the Group Policy Creators Owners role. The role can be defined for SVM users.
Remote Desktop Users	
IIS_IUSRS	
Replicator	
Offer Remote Assistance Helpers	

4 Protecting Data by Segregating Responsibilities

Using RBAC in clustered Data ONTAP leads to enhanced data protection through the concept of Segregation of Duties (SoD), or Separation of Duties, as it is also known. This concept prevents a single administrator from affecting access to data or other objects, such as logical interfaces, by limiting access using the principle of least privilege. The principle of least privilege simply states that a user or process should have the level of access required to perform his or her legitimate functions and no more. The principles of Segregation of Duties and the principle of least privilege are applied mostly in larger IT departments with distributed responsibilities, but smaller environments can take advantage of these features particularly with system accounts and the processes and functions they perform. These principles prevent a security incident on one system from spreading to others.

Following are to examples of how these concepts are applied using clustered Data ONTAP.

- Create a new role that allows a Windows administrator access to just the CIFS commands on a particular SVM to prevent that administrator from changing NFS configurations.
- Create a network administrator role at the cluster level that has access only to network commands. This role permits users to configure features such as DNS load-balancing without permitting those users to modify or even view data-container objects.

SoD is enforced by default in clustered Data ONTAP in several functional areas. An SVM administrator with the *vsadmin* role cannot perform volume move or LIF migrate operations, because those operations affect the load on individual hardware resources and can therefore affect the access that users of other SVMs have to those resources. For this reason the network administrator role in the example provided is defined at the cluster level and not at the SVM level.

Clustered Data ONTAP allows and, in some cases, enforces SoD through the various predefined SVM roles:

- The *vsadmin-readonly* role is used by auditors, and by definition they should have no access to make changes to operations.
- The *vsadmin-backup* role has access to all of the commands required to perform backups of an SVM and no more.
- The *vsadmin-protocol* role allows an administrator to perform functions at the data access layer, but the administrator is not able to modify data-container objects.

5 Design Considerations

This section focuses on the design considerations for creating the security policy for cluster and SVM users. Design considerations address the following environments:

- Existing Data ONTAP environments operating in 7-Mode
- New and existing clustered Data ONTAP environments

5.1 Existing Data ONTAP Operating in 7-Mode Environments

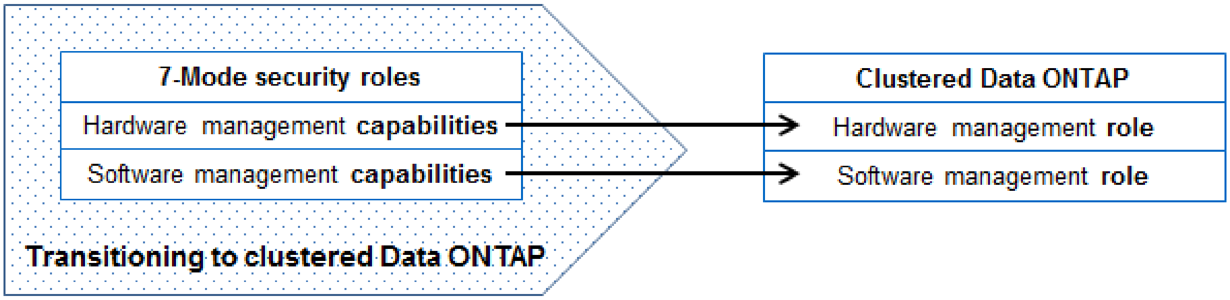
Data ONTAP operating in 7-Mode implements the following RBAC strategy: **A**ccounts are assigned to groups, **g**roups are assigned roles, and **r**oles are assigned **c**apabilities (A.G.R.C.).

Term	Description
Accounts	Users who interact with the administrative path of Data ONTAP. The two types of accounts are local account and domain user account. • Local: An account that is authenticated in Data ONTAP. • Domain user: A nonlocal user who belongs to a Windows domain and is authenticated by the domain.

Term	Description
Group	A collection of local and/or domain user accounts. Groups can be assigned one or more roles.
Role	A named set of capabilities.
Capabilities	A privilege that designates the task(s) a user can perform. Data ONTAP operating in 7-Mode supports the following capability types: login, cli, security, api, and compliance.

The primary focus for transitioning security roles from Data ONTAP operating in 7-Mode to clustered Data ONTAP is to separate the roles based on its scope. The following diagram illustrates how to analyze 7-Mode roles to determine if the role applies to a user who will administer a cluster or an SVM.

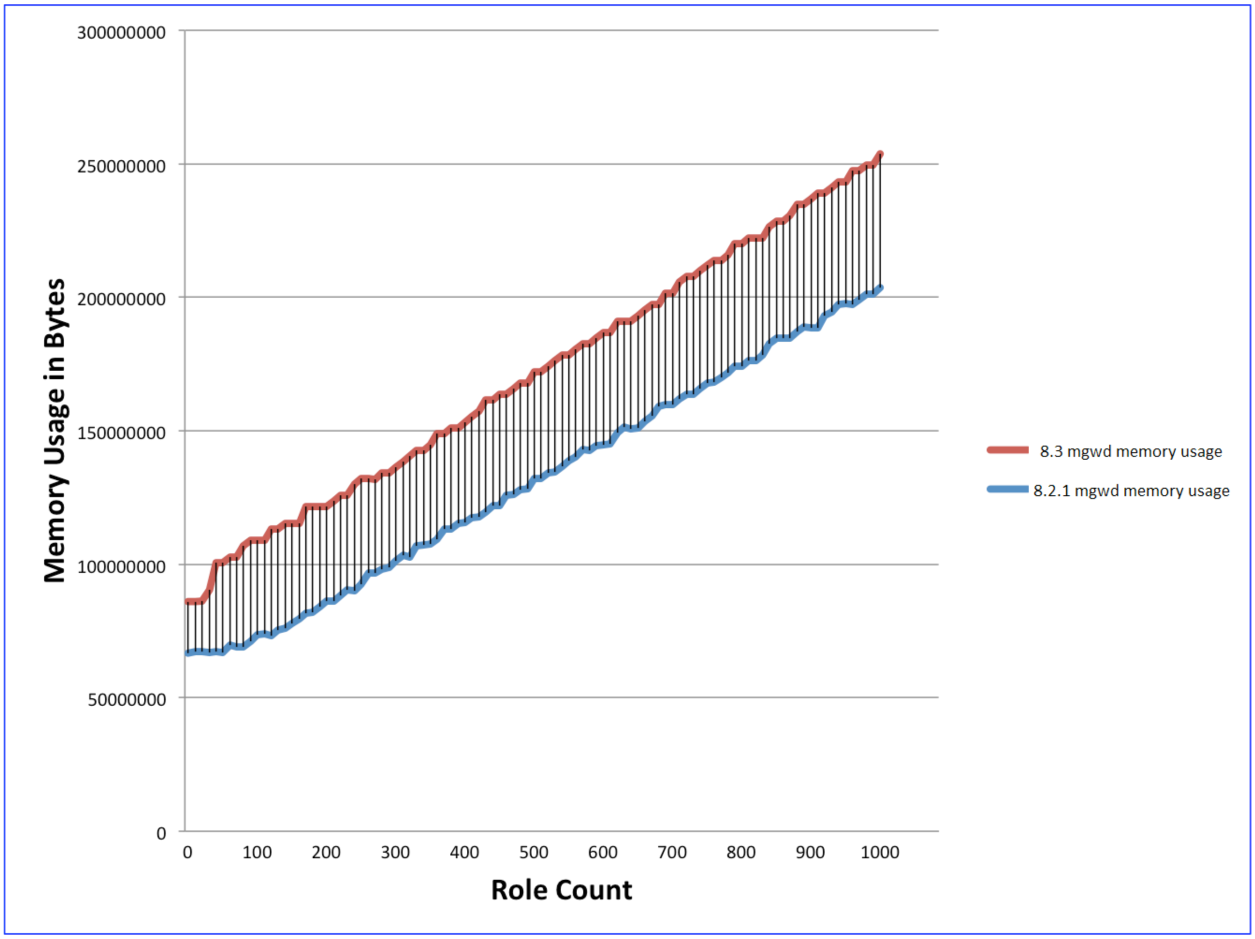
Figure 2) Transitioning 7-Mode security roles to clustered Data ONTAP roles.


7-Mode security roles
Hardware management capabilities
Software management capabilities
Transitioning to clustered Data ONTAP
Clustered Data ONTAP
Hardware management role
Software management role

5.2 New and Existing Clustered Data ONTAP Environments

Careful measurements by NetApp have shown that the number of custom roles in the cluster have a direct correlation to the memory consumed by the management daemon (mgwd), a design consideration for custom roles for cluster and SVM users. These tests show that although there is a cost (memory footprint) to creating custom roles for users on the cluster it should be balanced by the benefits of segregating user responsibilities on the cluster. The number of custom roles that provide this balance will vary based on the version of clustered Data ONTAP. Consult with your NetApp team to determine the level of customization that works best for your organization.

Figure 3) Correlation between number of roles and memory usage.



6 RBAC Implementation Planning

This table is a reference for specific versions of NetApp tools and indicates whether the versions support RBAC for logging into the tool itself or whether the tool supports RBAC when communicating with the storage cluster. This matrix provides an at-a-glance view of RBAC support of the solution as a whole.

Header Legend

- Tool-Specific MS AD Support: Ability to log into the tool using AD credentials instead of a local user.
- Tool-Specific RBAC Support: Ability to log into the tool using a non-admin role.
- Other***** MS AD RBAC Support: Tool can communicate with the storage cluster using Microsoft AD account with non-admin role.
- Other***** SVM RBAC Support: Tool can communicate with the storage virtual machine using non-admin role.
- Other***** Non-Admin Account Support: Tool can communicate with the storage cluster using a non-default-administrator role.

***Other** is defined as support between the clustered Data ONTAP cluster and third-party products, applications, and tools.

Table 5) RBAC tool matrix view by application.

Application	Tool-Specific MS AD Support	Tool-Specific RBAC Support	Other MS AD RBAC Support	Other SVM RBAC Support	Other Non-Admin-Account Support	RBAC User Creator Tool Support
Clustered Data ONTAP	N/A	N/A	Yes	Yes	Yes	No
NetApp Cluster-Interconnect Switch CN1610 1.1.0.4	No	No	N/A	N/A	N/A	No
NetApp Virtual Storage Console 5.0 VMware® vSphere®	Yes	Yes	Yes	No	Yes	Yes
NetApp Virtual Storage Console 4.2.1	Yes	No	Yes	No	Yes	Yes
NetApp SnapDrive® 7.0—Linux®	No	No	No	Yes	Yes	No
NetApp SnapDrive 7.0—Windows	N/A	No	Yes	Yes	Yes	No
NetApp SnapManager® 2.2	No	No	No	Yes	Yes	No

Application	Tool-Specific MS AD Support	Tool-Specific RBAC Support	Other MS AD RBAC Support	Other SVM RBAC Support	Other Non-Admin-Account Support	RBAC User Creator Tool Support
for Oracle						
NetApp SnapManager for MS-SQL 7.0	Yes	No	Yes	Yes	Yes	No
NetApp OCUM 6.1	Yes	Yes	Yes	No	Yes	No
NetApp OPM 1.0	Yes	No	Yes	No	Yes	No
NetApp OCC 5.2	Yes	No	Yes	No	Yes	No
NetApp AV Connector 1.0	N/A	No	Yes			No
Cisco® UCS® Director		Yes				No
VMware vCACs		Yes				N/A
VMware vCops vs. Blue Medora Monitoring Platform						N/A
NetApp WFA 2.2RC1	Yes	Yes	Yes	Yes	Yes	N/A
Custom Linux Scripts—SMO FlexClone® from SnapMirror Target	No	No	No	Yes	Yes	No
Symantec™ NetBackup™	Yes		Yes	No, planned	Yes	No

Table 6) RBAC tool matrix view by privileges.

Privilege	cDOT 8.2.2	SVM	OCUM 6.2	OPM 1.1	VSC 5.1	System Manager 3.0
RBAC User Creator Tool Support						
Local User Database	Yes	Yes	Yes	Yes	No	Yes
Local User Non-Admin Role Allowed	Yes	Yes			N/A	No?
Local User Customized Role Allowed	Yes	Yes			N/A	No?
MS-AD Authentication	Yes	Yes			Yes	Yes
MS-AD Non-Admin Authentication	Yes	Yes			Yes (vSphere 5.x)	No?
MS-AD Customized Role Authentication	Yes	Yes			Yes (vSphere 5.x)	No?
Tool->Storage Cluster MS-AD Authentication	N/A	N/A			Yes	Yes
Tool->Storage Cluster MS-AD Non-Admin Authentication	N/A	N/A			Yes	Maybe—untested
Tool->Storage Cluster MS-AD Customized Role Authentication	N/A	N/A			Yes	Maybe—untested
Tool->SVM MS-AD Authentication	N/A	N/A			Partial (backup requires cluster-wide priv)	No
Tool->SVM MS-AD Non-Admin Authentication	N/A	N/A			Partial (backup requires cluster-wide priv)	No
Tool->SVM MS-AD Customized Role Authentication	N/A	N/A			Partia (backup requires cluster-wide priv)	No
openLDAP Authentication						No
openLDAP Non-Admin Authentication						No
openLDAP Customized Role Authentication						No
Tool->Storage	N/A	N/A				No

Privilege	cDOT 8.2.2	SVM	OCUM 6.2	OPM 1.1	VSC 5.1	System Manager 3.0
Cluster openLDAP Authentication						
Tool->Storage Cluster openLDAP Non-Admin Authentication	N/A	N/A				No
Tool->Storage Cluster openLDAP Customized Role Authentication	N/A	N/A				No
Tool->SVM openLDAP Authentication	N/A	N/A				No
Tool->SVM openLDAP Non-Admin Authentication	N/A	N/A				No
Tool->SVM openLDAP Customized Role Authentication	N/A	N/A				No

7 Application Integration and Custom Roles

There are many instances in which you need to integrate NetApp products and third-party products, and those third-party products use a different access method. The ability to include specific commands and capabilities using custom roles allows clustered Data ONTAP to support a very diverse set of role-based access controls.

NetApp management products such as OnCommand® System Manager, OnCommand Unified Manager, OnCommand Workflow Automation, and many others utilize an access method known as the NetApp Manage ONTAP® storage development kit, formerly referred to as the NetApp ONTAPI® library. These management products are generally designed to manage clustered Data ONTAP or to perform specific functions. They typically make assumptions that the product has been given access to manage the solution using a higher-level admin account that has the scope and permission to manage the entire solution.

This section discusses the customization of clustered Data ONTAP roles using the Manage ONTAP framework.

Note: Custom roles defined for products that use the Manage ONTAP (ONTAPI) method need to be reevaluated when new versions of either clustered Data ONTAP or the integrated product are released. This is needed to confirm that the custom roles appropriately support any new capabilities that become available and that existing capabilities remain functional post-upgrade.

7.1 Custom Roles and Security Logins

Clustered Data ONTAP has several predefined default administration accounts such as `admin` for cluster management and `vsadmin` for storage virtual machine (SVM) management. These default logins use the Manage ONTAP application definition to define them as having either the *admin* role or the *vsadmin* role to give the login complete administrative control over that object.

The `security login create` command creates a login method for the management utility. A login method consists of a user name, an application (access method), and an authentication method. A user name can be associated with multiple applications. It can optionally include an access-control role name.

To see the set of security logins that are currently defined enter **`security login show`**.

```
cluster02::> security login show
Vserver: jd_nfs_test
                             Authentication                  Acct
UserName         Application Method         Role Name        Locked
---------------- ----------- -------------- ---------------- ------
vsadmin          ontapi      password       vsadmin          no
vsadmin          ssh         password       vsadmin          no

Vserver: source_wfa2_DR
                             Authentication                  Acct
UserName         Application Method         Role Name        Locked
---------------- ----------- -------------- ---------------- ------
vsadmin          ontapi      password       vsadmin          yes
vsadmin          ssh         password       vsadmin          yes

Vserver: cluster02
                             Authentication                  Acct
UserName         Application Method         Role Name        Locked
---------------- ----------- -------------- ---------------- ------
admin            console     password       admin            no
admin            http        password       admin            no
admin            ontapi      password       admin            no
admin            service-processor password admin            no
admin            ssh         password       admin            no
autosupport      console     password       autosupport      yes
lab\user1 ssh         domain         admin            -
lab\user2    ssh         domain         admin            -
public           snmp        community      readonly         -
13 entries were displayed.
```

To see the set of commands and access levels that a given role has defined enter **`security login role show`**.

```
cluster02::> security login role show
           Role          Command/                                      Access
Vserver    Name          Directory                               Query Level
---------- ------------- --------- ----------------------------------- --------
source_wfa2_DR       vsadmin       DEFAULT                                      none
source_wfa2_DR       vsadmin       dashboard health vserver
readonly
source_wfa2_DR       vsadmin       df
readonly
source_wfa2_DR       vsadmin       event generate-autosupport-log                all
source_wfa2_DR       vsadmin       job                                          all
source_wfa2_DR       vsadmin       job schedule
readonly
source_wfa2_DR       vsadmin       job schedule cron                            none
source_wfa2_DR       vsadmin       job schedule interval                        none
source_wfa2_DR       vsadmin       lun                                          all
source_wfa2_DR       vsadmin       network connections
readonly
source_wfa2_DR       vsadmin       network connections active show-clients       none
source_wfa2_DR       vsadmin       network connections active show-protocols     none
source_wfa2_DR       vsadmin       network connections active show-services      none
source_wfa2_DR       vsadmin       network interface
readonly
```

Although the *admin* role has full or complete access to all commands and directories in the cluster, the *vsadmin* role gives specific access to various commands and directories within the SVM.

Products such as OnCommand System Manager or OnCommand Unified Manager use these default security logins for the Manage ONTAP application. Both of these default login accounts have an ONTAPI application method defined. Most, if not all, of these management applications assume that their scope of management is complete and thus require access to all commands and directories.

The access levels available for definition in clustered Data ONTAP are *none*, *readonly,* and *all*. You can define an access level for a directory or command, and those definitions are inherited from the parent object. However, the net access level for a subdirectory or lower level in a command tree are cumulative, and if a more or less restrictive command is defined at a lower level it will still have an effect. For example, the *vsadmin* role has the command and *volume* directory tree set to a DEFAULT access level of *none* and then specific exceptions are added.

The same approach cannot be taken for applications such as the the OnCommand suite because they were designed to administer the cluster. First, define a role that has the command and directory tree set with a DEFAULT access level of *readonly* or *all*, depending on whether or not you want to specifically allow or deny a capability. This definition for the role allows these products and all other products that use the Manage ONTAP solution or ONTAPI application method to access the information in the cluster. Next, allow or deny access to specific commands and directories.

To begin, create a custom security role using the `security login role create` command.

```
cluster02::> security login role create ?
  [ -vserver <vserver name> ]  Vserver (default: cluster02)
   [-role] <text>              Role Name
   [-cmddirname] <text>        Command / Directory
  [[-access] <Access>]         Access Level (default: all)
  [ -query <query> ]           Query (default: "")
```

It is important to check if the custom role applies to the cluster or an SVM in the cluster. As an example, if you want to be very restrictive and allow only specific exceptions to commands, then define the DEFAULT access to the command tree to have the readonly access level and then define specific exceptions to allow operations such as volume creation. This method is demonstrated later with OnCommand System Manager.

To create a base custom role with restrictive readonly access enter:

```
cluster02::> security login role create -vserver cluster02 -role
MyCustomRole_defaultRestrictive -cmddirname DEFAULT -access readonly
```

```
cluster02::> security login role show -role MyCustomRole_defaultRestrictive
Role          Command/                                      Access

Vserver    Name          Directory                                        Query Level

---------- ------------- --------- ----------------------------------- --------

cluster02 MyCustomRole_defaultRestrictive DEFAULT               readonly
```

Now that a base role has been created to permit either full or readonly access, you can then tailor the directories and commands available to these roles. To do so, continue to add additional entries for the directories and commands you specifically desire to either restrict access to or allow access to.

To set the stage, the more restrictive custom role (MyCustomRole_defaultRestrictive) will be allowed to create NetApp FlexVol® volumes, but nothing else. The less restrictive role (MyCustomRole_defaultAll) will be able to administer all cluster objects, but it will be denied the ability to delete FlexVol volumes or take them offline.

To start with the more restrictive role that allows volume creation, enter the command shown below. Note that upon entering this command you are informed that this entry will also affect the `volume modify` and `volume show` commands. In this instance that is okay, but if it were not you would need to make additional entries to further tailor the role.

```
cluster02::> security login role create -vserver cluster02 -role
MyCustomRole_defaultRestrictive -cmddirname "volume create" -access all

Warning: This operation will also affect the following commands:
    "volume modify"
    "volume show"
cluster02::> security login role show -role MyCustomRole_defaultRestrictive
Role          Command/                                     Access
Vserver    Name          Directory                               Query Level
---------- ------------- --------- ----------------------------------- --------
cluster02 MyCustomRole_defaultRestrictive DEFAULT               readonly
cluster02 MyCustomRole_defaultRestrictive volume create         all
cluster02 MyCustomRole_defaultRestrictive volume modify         all
cluster02 MyCustomRole_defaultRestrictive volume show           all
4 entries were displayed.
```

If you want to be less restrictive and allow a broader set of capabilities but then later specifically deny certain commands such as `volume deletion`, then define the DEFAULT command with the *all* access level. This method will be demonstrated later with OnCommand System Manager.

To create a base custom role with full access enter the following command:

```
cluster02::> security login role create -vserver cluster02 -role
MyCustomRole_defaultAll -cmddirname DEFAULT -access all

cluster02::> security login role show -role MyCustomRole_defaultAll
           Role          Command/                                      Access
Vserver    Name          Directory                               Query Level
---------- ------------- --------- ----------------------------------- --------
cluster02 MyCustomRole_defaultAll DEFAULT                       all
```

Next we will modify the custom role that has full capabilities by default and restrict that role from deleting FlexVol volumes or taking them offline. Start by entering the following command:

```
cluster02::> security login role create -vserver cluster02 -role
MyCustomRole_defaultAll -cmddirname "volume delete" -access none

cluster02::> security login role create -vserver cluster02 -role
MyCustomRole_defaultAll -cmddirname "volume offline" -access none

cluster02::> security login role show
    show        show-ontapi
cluster02::> security login role show -role MyCustomRole_defaultAll
           Role          Command/                                      Access
Vserver    Name          Directory                               Query Level
---------- ------------- --------- ----------------------------------- --------
cluster02
           MyCustomRole_defaultAll
                         DEFAULT                                       all
cluster02
           MyCustomRole_defaultAll
                         volume delete                                 none
cluster02
           MyCustomRole_defaultAll
                         volume offline                                none
3 entries were displayed.
```

After the custom roles have been defined, you next need to create some security logins to use these roles. These logins will only have the application method of Manage ONTAP or ONTAPI defined. We will demonstrate these custom roles using OnCommand System Manager with Active Directory–based logins.

To create a security login for the restrictive role that only allows volume creation enter:

```
cluster02::> security login create -vserver cluster02 -user netapp\OnlyVolumeCreate -
application ontapi -authmethod domain -role MyCustomRole_defaultRestrictive

cluster02::> security login show -vserver cluster02

Vserver: cluster02
                             Authentication                  Acct
User/Group Name  Application Method         Role Name        Locked
```

```
---------------- ----------- -------------- ---------------- ------
netapp\OnlyVolumeCreate ontapi      domain       MyCustomRole_defaultRestrictive
                                                             no
admin            console     password       admin            no
admin            http        password       admin            no
admin            ontapi      password       admin            no
admin            service-processor
                             password       admin            no
admin            ssh         password       admin            no
autosupport      console     password       autosupport      no
7 entries were displayed.
```

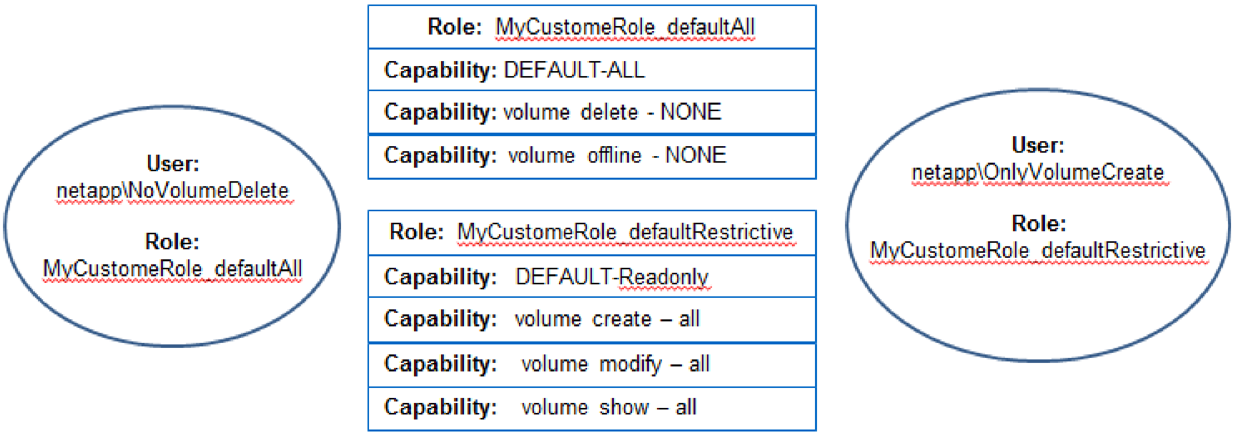
To create a security login for the less restrictive role that allows everything except for volume deletion enter:

```
cluster02::> security login create -vserver cluster02 -user netapp\NoVolumeDelete -
application ontapi -authmethod domain -role MyCustomRole_defaultAll
cluster02::> security login show -vserver cluster02

Vserver: cluster02
                             Authentication                  Acct
User/Group Name  Application Method         Role Name        Locked
---------------- ----------- -------------- ---------------- ------
netapp\NoVolumeDelete ontapi      domain       MyCustomRole_defaultAll
                                                             no
admin            console     password       admin            no
admin            http        password       admin            no
admin            ontapi      password       admin            no
admin            service-processor
                             password       admin            no
admin            ssh         password       admin            no
autosupport      console     password       autosupport      no
7 entries were displayed.
```

7.2 Demonstration of Custom Roles Using OnCommand System Manager

This section demonstrates the custom roles and security logins created in the previous section using OnCommand System Manager.

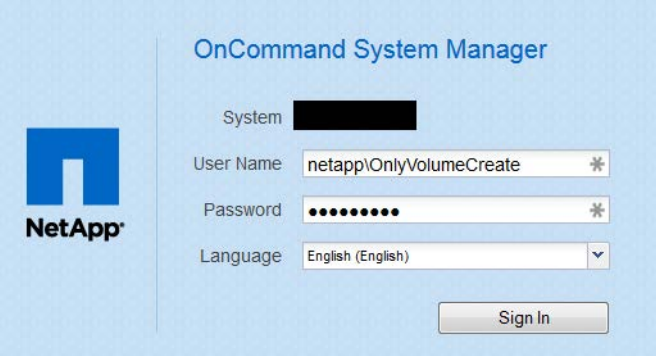
Figure 4) Example of using custom roles with OnCommand System Manager.


User:
netapp\NoVolumeDelete
Role:
MyCustomeRole_defaultAll
Role: MyCustomeRole_defaultAll
Capability: DEFAULT-ALL
Capability: volume delete - NONE
Capability: volume offline - NONE
Role: MyCustomeRole_defaultRestrictive
Capability: DEFAULT-Readonly
Capability: volume create – all
Capability: volume modify – all
Capability: volume show – all
User:
netapp\OnlyVolumeCreate
Role:
MyCustomeRole_defaultRestrictive

7.2.1 Readonly Role with Volume Creation

Here we demonstrate that the netapp\OnlyVolumeCreate user has only the capability to create FlexVol volumes.

We will log in with the netapp\OnlyVolumeCreate user.



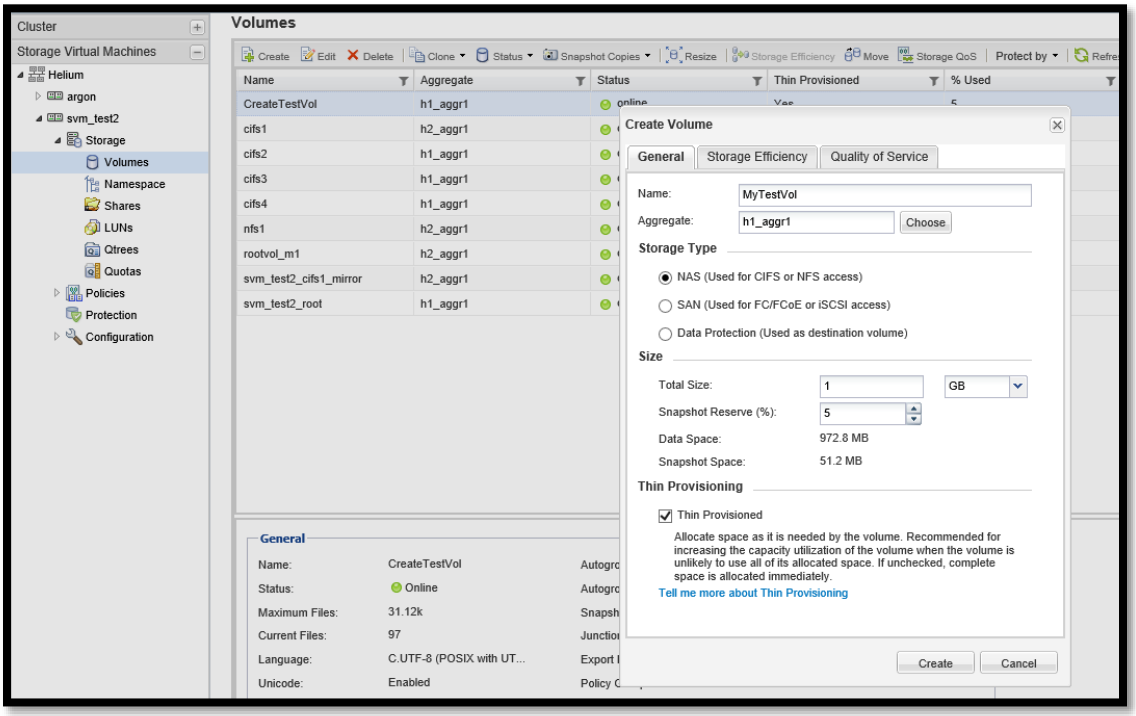
System: [redacted]

User Name: netapp\OnlyVolumeCreate

Password: ●●●●●●●●●

Language: English (English)

Next we navigate to the appropriate SVM and create a NAS FlexVol volume.



Name	Aggregate	Status	Thin Provisioned	% Used
CreateTestVol	h1_aggr1	online	Yes	5
cifs1	h2_aggr1			
cifs2	h1_aggr1			
cifs3	h1_aggr1			
cifs4	h1_aggr1			
nfs1	h2_aggr1			
rootvol_m1	h2_aggr1			
svm_test2_cifs1_mirror	h2_aggr1			
svm_test2_root	h1_aggr1			

General

Name: CreateTestVol

Status: Online

Maximum Files: 31.12k

Current Files: 97

Language: C.UTF-8 (POSIX with UT...

Unicode: Enabled

Create Volume

General | Storage Efficiency | Quality of Service

Name: MyTestVol

Aggregate: h1_aggr1 Choose

Storage Type

● NAS (Used for CIFS or NFS access)

○ SAN (Used for FC/FCoE or iSCSI access)

○ Data Protection (Used as destination volume)

Size

Total Size: 1 GB

Snapshot Reserve (%): 5

Data Space: 972.8 MB

Snapshot Space: 51.2 MB

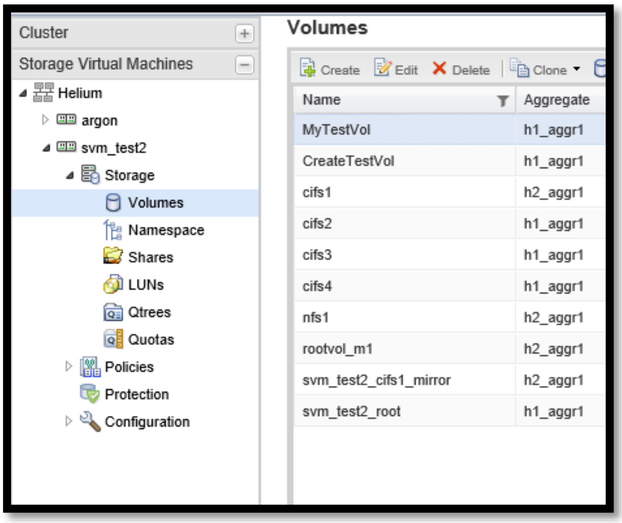
Thin Provisioning

☑ Thin Provisioned

Allocate space as it is needed by the volume. Recommended for increasing the capacity utilization of the volume when the volume is unlikely to use all of its allocated space. If unchecked, complete space is allocated immediately.

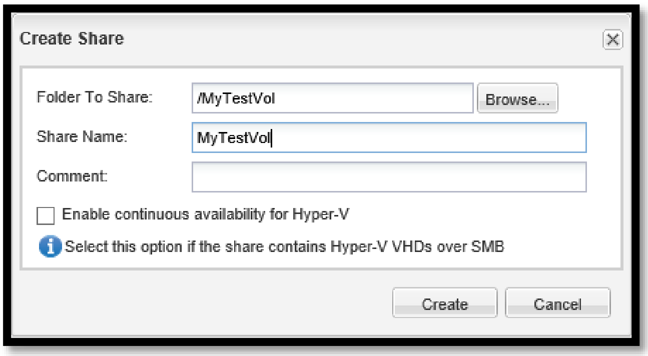
Tell me more about Thin Provisioning

This command succeeds and mounts the volume to the namespace.



Name	Aggregate
MyTestVol	h1_aggr1
CreateTestVol	h1_aggr1
cifs1	h2_aggr1
cifs2	h1_aggr1
cifs3	h1_aggr1
cifs4	h1_aggr1
nfs1	h2_aggr1
rootvol_m1	h2_aggr1
svm_test2_cifs1_mirror	h2_aggr1
svm_test2_root	h1_aggr1

We then try to share the FlexVol volume using CIFS, which fails.



Create Share

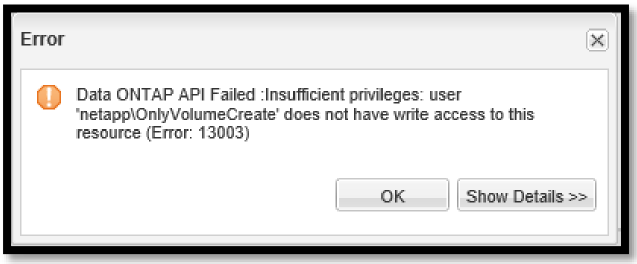
Folder To Share: /MyTestVol

Share Name: MyTestVol

Comment:

□ Enable continuous availability for Hyper-V

Select this option if the share contains Hyper-V VHDs over SMB



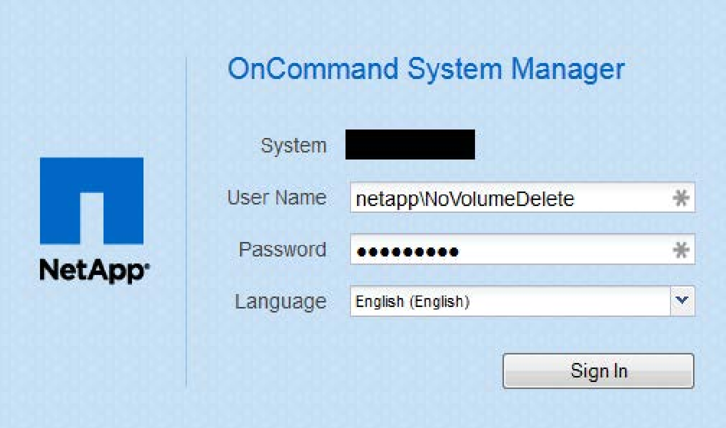
Error

Data ONTAP API Failed :Insufficient privileges: user 'netapp\OnlyVolumeCreate' does not have write access to this resource (Error: 13003)

7.2.2 Full Access Role with Volume Deletion Denied

Here we demonstrate that netapp\NoVolumeDelete user has the capability to do everything except delete volumes or take them offline.

We log in with the netapp\OnlyVolumeCreate user.



OnCommand System Manager

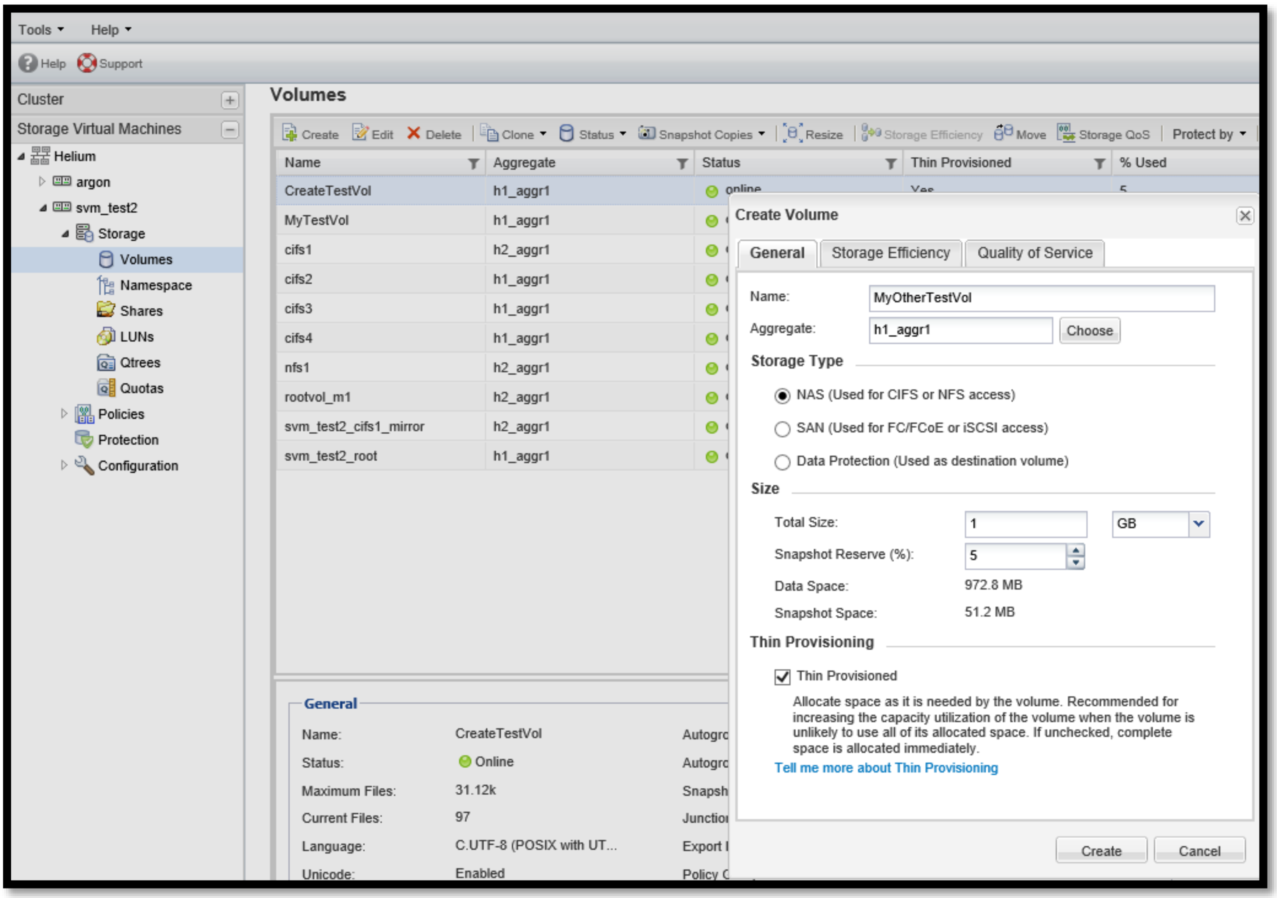
System [redacted]

User Name netapp\NoVolumeDelete

Password ●●●●●●●●●

Language English (English)

We create a new FlexVol volume with the name MyOtherTestVol.



Name	Aggregate	Status	Thin Provisioned	% Used
CreateTestVol	h1_aggr1	online	Yes	5
MyTestVol	h1_aggr1			
cifs1	h2_aggr1			
cifs2	h1_aggr1			
cifs3	h1_aggr1			
cifs4	h1_aggr1			
nfs1	h2_aggr1			
rootvol_m1	h2_aggr1			
svm_test2_cifs1_mirror	h2_aggr1			
svm_test2_root	h1_aggr1			

General

Name:	CreateTestVol	Autogro
Status:	● Online	Autogro
Maximum Files:	31.12k	Snapsh
Current Files:	97	Junctio
Language:	C.UTF-8 (POSIX with UT...	Export I
Unicode:	Enabled	Policy C

Create Volume

General | Storage Efficiency | Quality of Service

Name: MyOtherTestVol

Aggregate: h1_aggr1 Choose

Storage Type

● NAS (Used for CIFS or NFS access)

○ SAN (Used for FC/FCoE or iSCSI access)

○ Data Protection (Used as destination volume)

Size

Total Size: 1 GB

Snapshot Reserve (%): 5

Data Space: 972.8 MB

Snapshot Space: 51.2 MB

Thin Provisioning

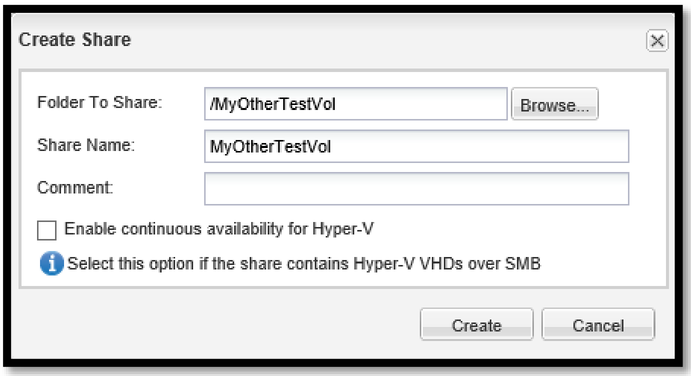
☑ Thin Provisioned

Allocate space as it is needed by the volume. Recommended for increasing the capacity utilization of the volume when the volume is unlikely to use all of its allocated space. If unchecked, complete space is allocated immediately.

Tell me more about Thin Provisioning

Create Cancel

We then share this volume through CIFS.



Create Share

Folder To Share: /MyOtherTestVol Browse...

Share Name: MyOtherTestVol

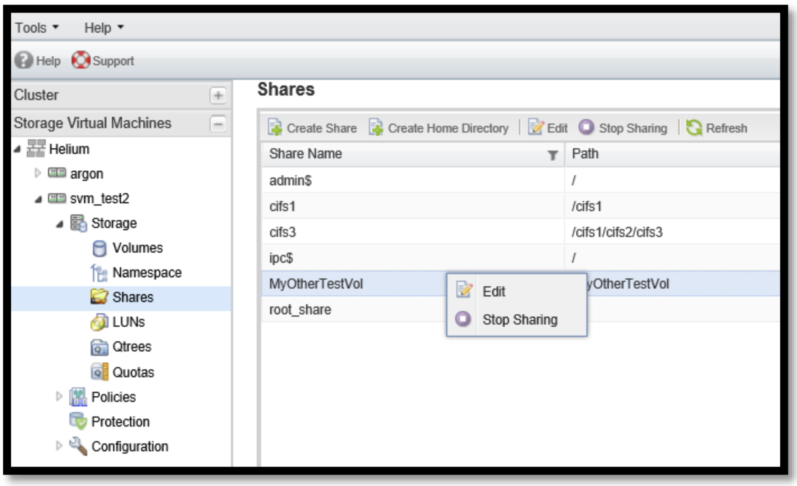
Comment:

□ Enable continuous availability for Hyper-V

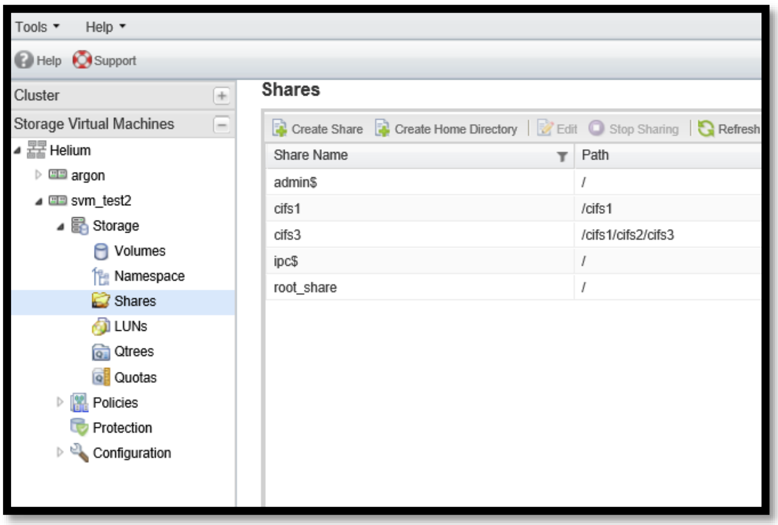
Select this option if the share contains Hyper-V VHDs over SMB

Create Cancel

Now let’s assume that you no longer need this FlexVol volume and wish to remove it. Go to Shares, select the volume, and right-click to Stop Sharing the l volume. The command succeeds.

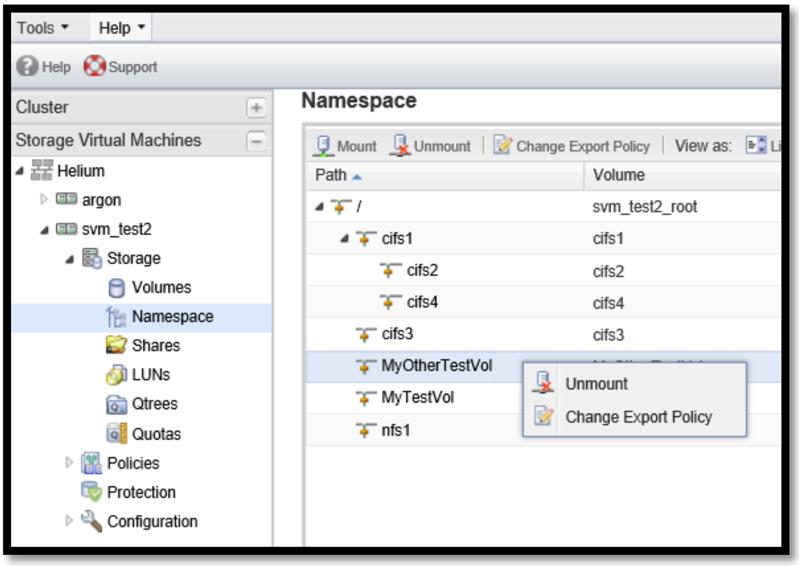


Share Name	Path
admin$	/
cifs1	/cifs1
cifs3	/cifs1/cifs2/cifs3
ipc$	/
MyOtherTestVol	yOtherTestVol
root_share	



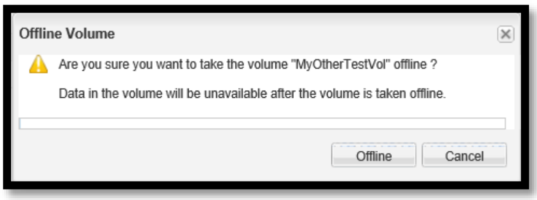
Share Name	Path
admin$	/
cifs1	/cifs1
cifs3	/cifs1/cifs2/cifs3
ipc$	/
root_share	/

Next, unmount the volume.



Path	Volume
/	svm_test2_root
cifs1	cifs1
cifs2	cifs2
cifs4	cifs4
cifs3	cifs3
MyOtherTestVol	
MyTestVol	
nfs1	

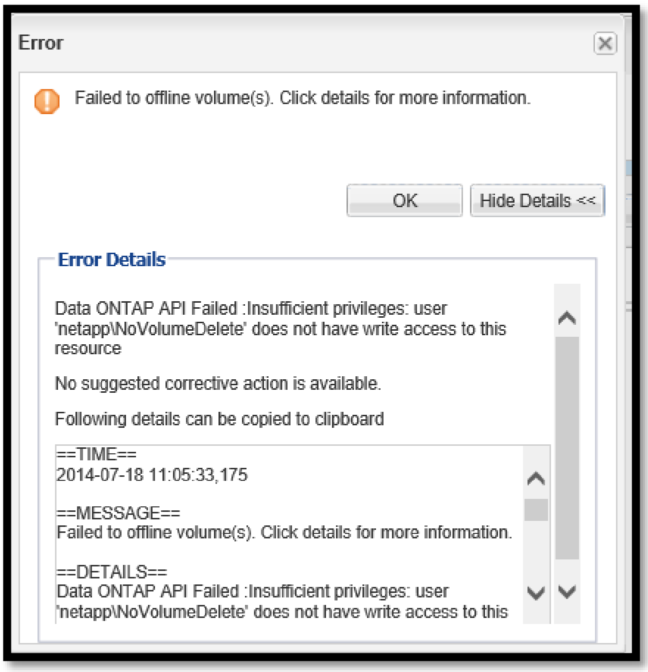
Then set the volume to offline. After asking you to confirm your action, the system responds with an error because the user does not have permission to take that action.



Offline Volume

Are you sure you want to take the volume "MyOtherTestVol" offline ?

Data in the volume will be unavailable after the volume is taken offline.



Error

Failed to offline volume(s). Click details for more information.

Error Details

Data ONTAP API Failed :Insufficient privileges: user 'netapp\NoVolumeDelete' does not have write access to this resource

No suggested corrective action is available.

Following details can be copied to clipboard

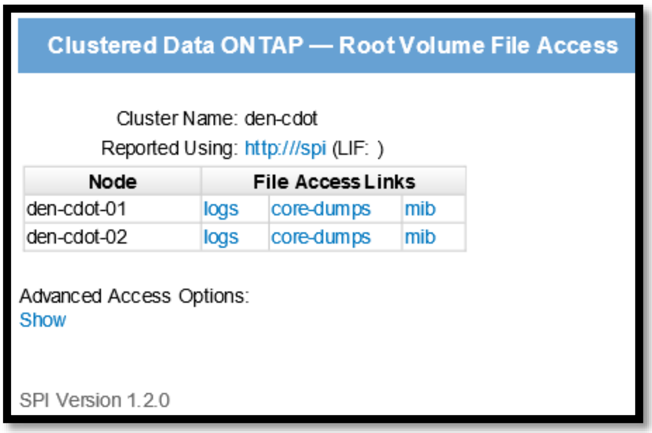
```
==TIME==
2014-07-18 11:05:33,175

==MESSAGE==
Failed to offline volume(s). Click details for more information.

==DETAILS==
Data ONTAP API Failed :Insufficient privileges: user
'netapp\NoVolumeDelete' does not have write access to this
```

7.3 Determining Required Permissions, Directories, and Commands

Many products that integrate with clustered Data ONTAP, including both NetApp products and third-party products, do not document the minimum required set of directories and commands that are required for the product to function with clustered Data ONTAP. The only method available to determine the minimum required directory and/or command list required is trial and error. Fortunately we can use some of our native auditing tools to assist us. For reference review NetApp Knowledge Base article KB3014168.

7.3.1 SPI Web Interface

The Service Processor Infrastructure (SPI) web interface is a method of enabling access to a cluster or node's log files from a browser and is described in the "Data ONTAP 8.3 System Administration Guide for Cluster Administrators." Note that the SPI web interface is enabled by default in clustered Data ONTAP 8.3.



Clustered Data ONTAP — Root Volume File Access

Cluster Name: den-cdot

Reported Using: http:///spi (LIF:)

Node	File Access Links		
den-cdot-01	logs	core-dumps	mib
den-cdot-02	logs	core-dumps	mib

Advanced Access Options:
Show

SPI Version 1.2.0

Navigate to `<nodename>/logs/mlog/command-history.log` and open the file to review any access-denied messages. This will obviously be more challenging on active or production clusters.

```
0000000f.0016ae1b 03cfc1b7 Mon Aug 18 2014 13:51:06 +01:00 [kern_command-
history:info:974] ssh :: 10.68.56.193 :: admin :: security login role create -vserver
```

```
sptech-cluster02 -role MyCustomRole_defaultAll -cmddirname DEFAULT -access all ::
Pending

0000000f.0016ae1d 03cfc1b7 Mon Aug 18 2014 13:51:06 +01:00 [kern_command-
history:info:974] ssh :: 10.68.56.193 :: admin :: security login role create -vserver
sptech-cluster02 -role MyCustomRole_defaultAll -cmddirname DEFAULT -access all ::
Success

0000000f.0016ae48 03cfc454 Mon Aug 18 2014 13:52:13 +01:00 [kern_command-
history:info:974] ssh :: 10.68.56.193 :: admin :: security login role create -vserver
sptech-cluster02 -role MyCustomRole_defaultAll -cmddirname DEFAULT -access all ::
Pending

0000000f.0016ae4b 03cfc454 Mon Aug 18 2014 13:52:13 +01:00 [kern_command-
history:info:974] ssh :: 10.68.56.193 :: admin :: security login role create -vserver
sptech-cluster02 -role MyCustomRole_defaultAll -cmddirname DEFAULT -access all ::
Error: duplicate entry
```

Note that the SPI web interface is not available on clustered Data ONTAP simulators.

From here there is nothing more to do than use the product and, upon feature failure, review the *command-history.log* files to determine the appropriate command or directory with which to enable your default-restricted role.

7.4 Demonstration of Custom Roles Using OnCommand Unified Manager and OnCommand Performance Manager

This section provides the clustered Data ONTAP 8.3 commands used for creating roles and users using OnCommand Unified Manager 6.2 and OnCommand Performance Manager. The role must support the following features:

- All the usual monitoring abilities of Unified Manager
- Allow NetApp SnapRestore® technology to function for restores within the same volume (production cluster)
- Allow NDMP restore from other volumes (for example, from SnapVault clusters or disaster recovery clusters)

7.4.1 Prerequisites

The role requires that the command `vserver services ndmp` is turned on for the cluster to enable NDMP restores to work.

The command shown here checks and enables NDMP services on the SVM:

```
cluster02::> vserver services ndmp show -vserver cluster02 -fields enable
cluster02::> vserver services ndmp on -vserver cluster02
```

Creating a user called ocum for Unified Manager that can also turn NDMP on results in a relatively unrestricted account:

```
UserName   Application Method   Role Name
---------- ----------- -------- ---------
ocum       console     password admin
ocum       ontapi      password admin
ocum       ssh         password backup
```

7.4.2 Creating the OnCommand Unified Manager Role

The commands below create a role called ocum:

```
cluster02::> security login role create -role ocum -cmddirname DEFAULT -
access readonly

cluster02::> security login role create -role ocum -cmddirname "volume file
show-disk-usage" -access all
```

```
cluster02::> security login role create -role ocum -cmddirname "volume
snapshot restore-file" -access all
```

```
cluster02::> security login role create -role ocum -cmddirname "storage
aggregate check_spare_low" -access all
```

```
cluster02::> security login role create -role ocum -cmddirname "storage disk
show" -access all
```

Command lines 1 and 2 are required by OnCommand Unified Manager for monitoring. Command line 4 was added because we saw an alert for `aggr-check-spare-low` with Insufficient privileges in the command-history.log.

The second and third lines are required for SnapRestore functionality to work correctly.

Line 5 was added because we saw an error from `storage-shelf-list-info` in the command-history.log with Enclosure services not ready at this time. Adding `storage disk show all` also affects storage disk modify.

7.4.3 Creating the OnCommand Unified Manager User

The commands below create a user called ocum:

```
cluster02::> security login create -username ocum -application ontapi -role
ocum -authmethod password
```

```
cluster02::> security login create -username ocum -application ssh -role
backup -authmethod password
```

The second line is required because only users with application ssh and the role *admin* or *backup* can run the command `vserver services ndmp generate-password`, which is required for NDMP restores to function (also the backup role comes with `vserver services ndmp` all access).

7.4.4 Creating the OnCommand Performance Manager Role

The commands below create a role called opm for OnCommand Performance Manager:

```
cluster02::> security login role create -role opm -cmddirname DEFAULT -access
readonly
```

```
cluster02::> security login role create -role opm -cmddirname "cluster
application-record" -access all
```

```
cluster02::> security login role create -role opm -cmddirname "volume modify"
-access all
```

```
cluster02::> security login role create -role opm -cmddirname "storage disk
show" -access all
```

The role is constructed by resolving clustered Data ONTAP errors as seen in the command-history.log. Insufficient privileges errors were seen for `cluster-application-record-create`, `volume-modify-iter`, and `storage-shelf-list-info`. Adding `volume modify` all also effects `volume create` and `volume show`. Adding `storage disk show` all also affects `storage disk modify`.

7.4.5 Creating the OnCommand Performance Manager User

The command below creates a user called opm:

```
cluster02::> security login create -username opm -application ontapi -role
opm -authmethod password
```

7.4.6 Outputs for OnCommand Unified Manager User and Roles

The commands below show the user called ocum and its role:

```
cluster02::> security login role show -role ocum

Role          Command/                                      Access
Name          Directory                               Query Level
------------- --------- ----------------------------------- --------
ocum          DEFAULT                                       readonly
ocum          storage aggregate check_spare_low             all
ocum          storage disk modify                           all
ocum          storage disk show                             all
ocum          volume file show-disk-usage                   all
ocum          volume snapshot restore-file                  all
6 entries were displayed.

cluster02::> security login role show -role backup

Role          Command/                                      Access
Name          Directory                               Query Level
------------- --------- ----------------------------------- --------
backup        DEFAULT                                       none
backup        volume                                        readonly
backup        vserver services ndmp                         all
3 entries were displayed.


cluster02::> security login show -user ocum

                             Authentication                  Acct
UserName         Application Method         Role Name        Locked
---------------- ----------- -------------- ---------------- ------
ocum             ontapi      password       ocum             no
ocum             ssh         password       backup           no
2 entries were displayed.
```

Note: Backup is a default role and cannot be modified.

7.4.7 Outputs for OnCommand Performance Manager User and Roles

The commands below show the user called ocum and its role:

```
cluster02::> security login role show -role opm

Role          Command/                                      Access
Name          Directory                               Query Level
------------- --------- ----------------------------------- --------
opm          DEFAULT                                       readonly
opm          cluster application-record                    all
opm          storage disk modify                           all
opm          storage disk show                             all
opm          volume create                                 all
opm          volume modify                                 all
opm          volume show                                   all
7 entries were displayed.

cluster02::> security login show -user opm

                             Authentication                  Acct
UserName         Application Method         Role Name        Locked
---------------- ----------- -------------- ---------------- ------
opm             ontapi      password       opm             no
```

8 RBAC User Creator

Use the application RBAC User Creator for clustered Data ONTAP to easily create both roles and users for common applications. Currently version 2.7 of RBAC User Creator creates Data ONTAP users and roles for the following applications:

- Virtual Storage Console for VMware vSphere (4.0, 4.1, 4.2, 4.2.1, and 5.0)
- NetApp Snap Creator® Framework (3.6.0 and 4.0.0)
- SnapDrive for Windows (6.4.2)
- Storage Replication Adapter for VMware vCenter™ Site Recovery Manager™ (2.1)
- Virtual Storage Console for Citrix XenServer (2.0 and 2.0.1)
- Virtual Storage Console for Red Hat Enterprise Virtualization (1.0)
- NetApp Recovery Manager for Citrix ShareFile (1.0)
- VMTurbo Operations Manager (2.0)
- OnCommand Balance
- SnapDrive for Windows

RBAC User Creator requires a Windows host to run. The RBAC User Creator tool is a free tool located in the NetApp MySupport Toolchest. It is supported on a best-effort volunteer basis through the communities: https://communities.netapp.com/docs/DOC-19074.

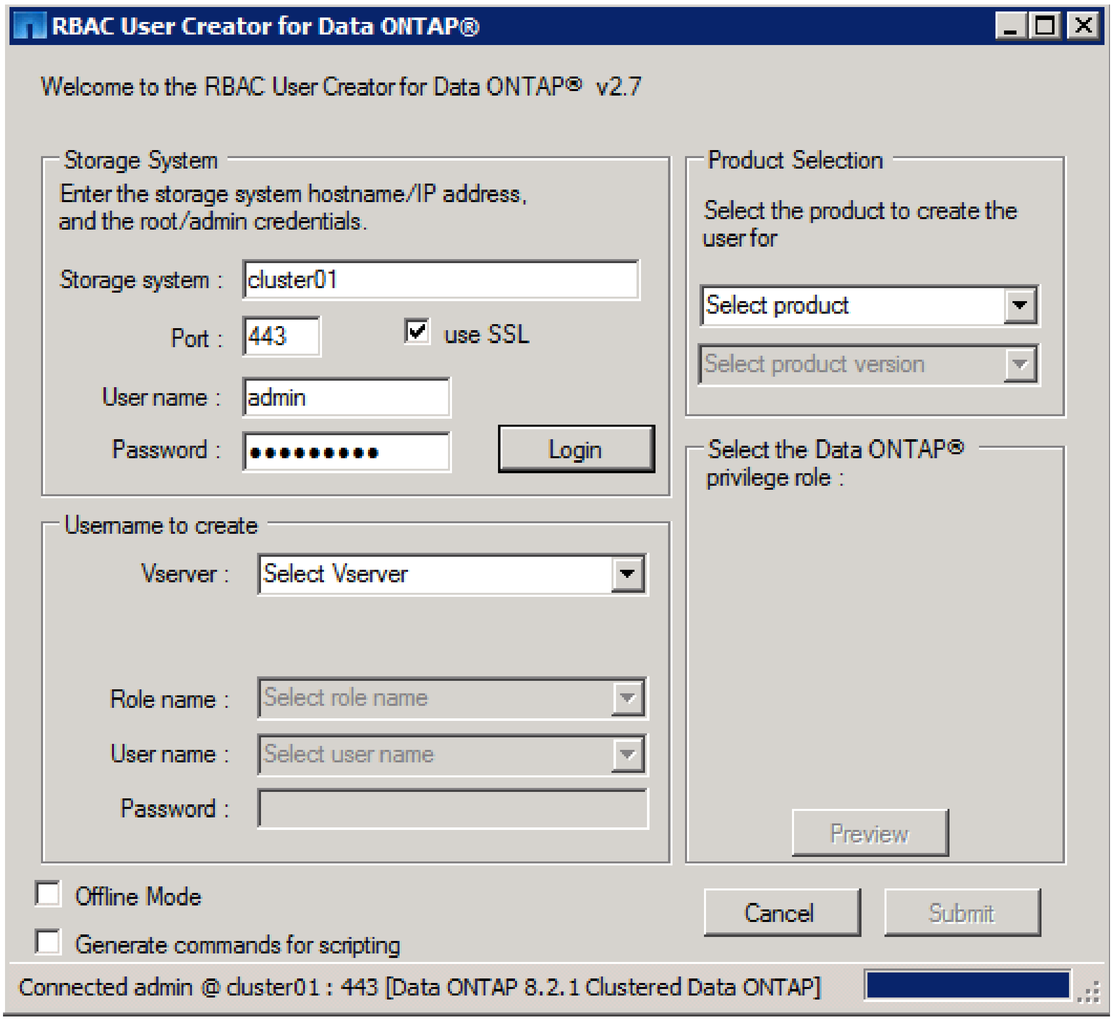
The RBAC User Creator tool was created to reduce error and improve the speed of provisioning of custom application-based roles for the NetApp Virtual Storage Console. The tool is structured to support extensible updates by the end user with an XML-based INI file.

Because of this flexibility, numerous precreated roles are defined in the current release of the RBAC User Creator tool. It is important to note that this tool supports both Data ONTAP systems operating in 7-Mode and clustered Data ONTAP systems. Some roles, such as DFM 5.2, are only for Data ONTAP systems operating in 7-Mode and will fail to provision against clustered Data ONTAP systems. This can be explicitly validated by reviewing the easy-to-read INI files.

The following section provides an example workflow of provisioning an SVM-specific role for Virtual Storage Console 4.2.1 with clustered Data ONTAP 8.3.

8.1.1 Creating a Custom Role from the Graphical User Interface (GUI)

1. Enter the admin credentials for the cluster and click **Login**.



RBAC User Creator for Data ONTAP®

Welcome to the RBAC User Creator for Data ONTAP® v2.7

Storage System

Enter the storage system hostname/IP address, and the root/admin credentials.

Storage system : cluster01

Port : 443 ☑ use SSL

User name : admin

Password : ●●●●●●●●●●

Username to create

Vserver : Select Vserver

Role name : Select role name

User name : Select user name

Password :

Product Selection

Select the product to create the user for

Select product

Select product version

Select the Data ONTAP® privilege role :

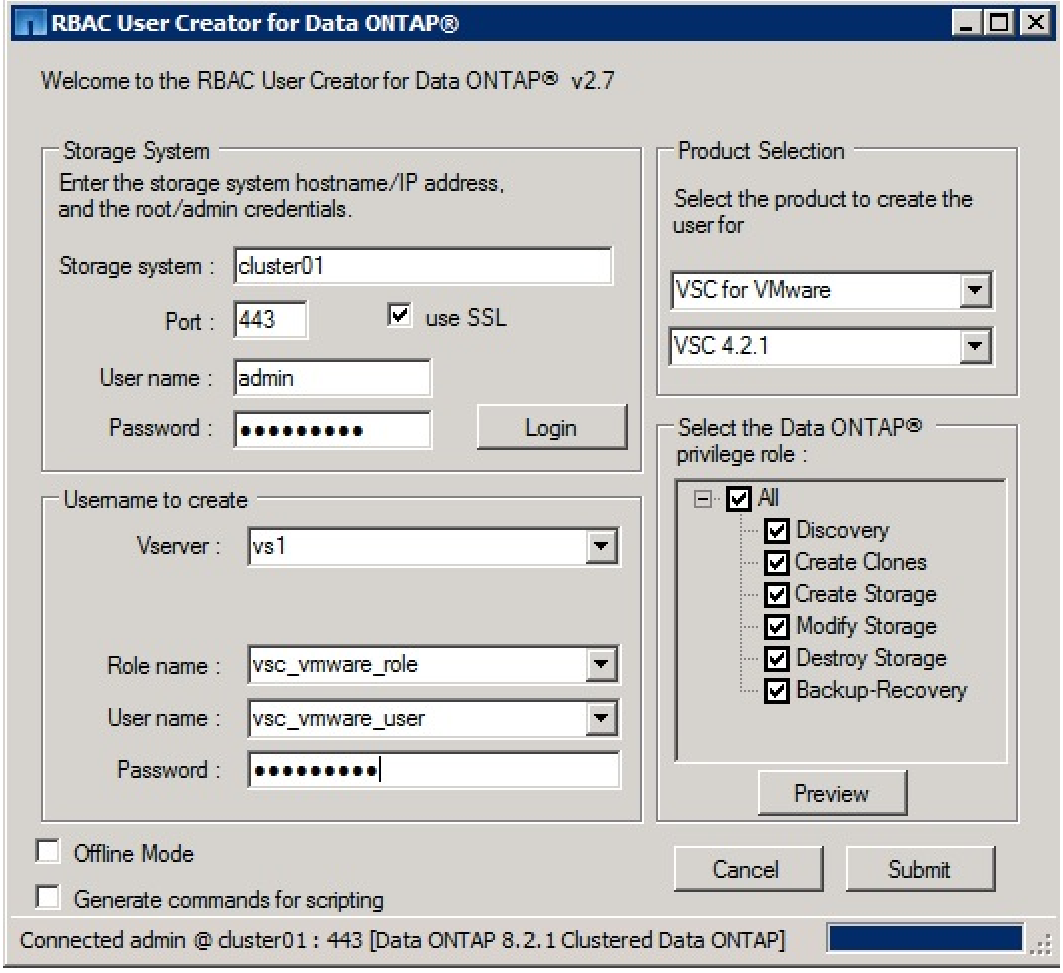
☐ Offline Mode

☐ Generate commands for scripting

Connected admin @ cluster01 : 443 [Data ONTAP 8.2.1 Clustered Data ONTAP]

2. Select the product, version, and capabilities in the right-hand pane.
3. Choose the storage virtual machine (formerly known as Vserver) and enter text for the new role name and the new user name.

   Note: Do not press the drop-down for role name and user name. Enter new text here.



RBAC User Creator for Data ONTAP®

Welcome to the RBAC User Creator for Data ONTAP® v2.7

Storage System

Enter the storage system hostname/IP address, and the root/admin credentials.

Storage system : cluster01

Port : 443 ☑ use SSL

User name : admin

Password : ●●●●●●●●●

Username to create

Vserver : vs1

Role name : vsc_vmware_role

User name : vsc_vmware_user

Password : ●●●●●●●●●●

Product Selection

Select the product to create the user for

VSC for VMware

VSC 4.2.1

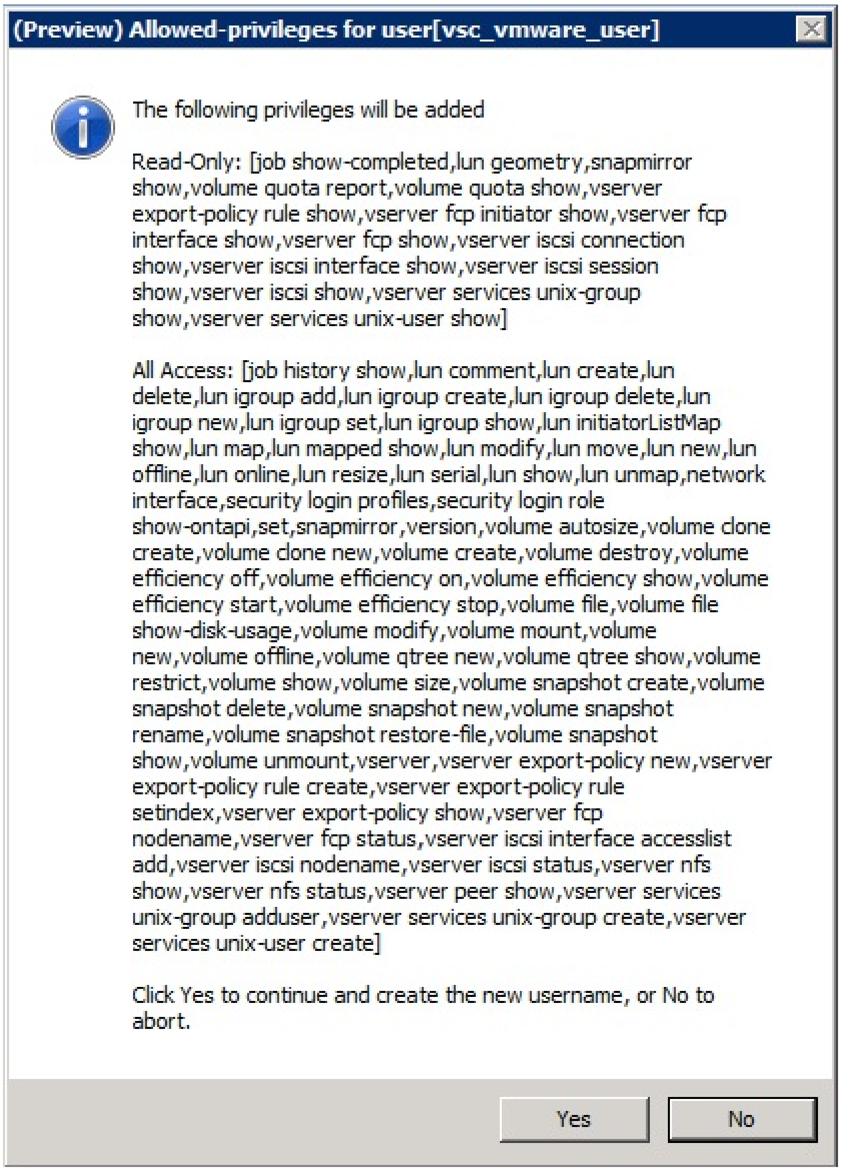
Select the Data ONTAP® privilege role :

- ☑ All
  - ☑ Discovery
  - ☑ Create Clones
  - ☑ Create Storage
  - ☑ Modify Storage
  - ☑ Destroy Storage
  - ☑ Backup-Recovery

□ Offline Mode

□ Generate commands for scripting

Connected admin @ cluster01 : 443 [Data ONTAP 8.2.1 Clustered Data ONTAP]



(Preview) Allowed-privileges for user[vsc_vmware_user]

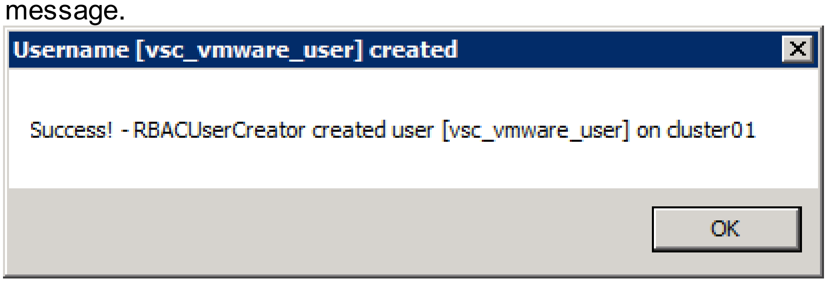
The following privileges will be added

Read-Only: [job show-completed,lun geometry,snapmirror show,volume quota report,volume quota show,vserver export-policy rule show,vserver fcp initiator show,vserver fcp interface show,vserver fcp show,vserver iscsi connection show,vserver iscsi interface show,vserver iscsi session show,vserver iscsi show,vserver services unix-group show,vserver services unix-user show]

All Access: [job history show,lun comment,lun create,lun delete,lun igroup add,lun igroup create,lun igroup delete,lun igroup new,lun igroup set,lun igroup show,lun initiatorListMap show,lun map,lun mapped show,lun modify,lun move,lun new,lun offline,lun online,lun resize,lun serial,lun show,lun unmap,network interface,security login profiles,security login role show-ontapi,set,snapmirror,version,volume autosize,volume clone create,volume clone new,volume create,volume destroy,volume efficiency off,volume efficiency on,volume efficiency show,volume efficiency start,volume efficiency stop,volume file,volume file show-disk-usage,volume modify,volume mount,volume new,volume offline,volume qtree new,volume qtree show,volume restrict,volume show,volume size,volume snapshot create,volume snapshot delete,volume snapshot new,volume snapshot rename,volume snapshot restore-file,volume snapshot show,volume unmount,vserver,vserver export-policy new,vserver export-policy rule create,vserver export-policy rule setindex,vserver export-policy show,vserver fcp nodename,vserver fcp status,vserver iscsi interface accesslist add,vserver iscsi nodename,vserver iscsi status,vserver nfs show,vserver nfs status,vserver peer show,vserver services unix-group adduser,vserver services unix-group create,vserver services unix-user create]

Click Yes to continue and create the new username, or No to abort.

Allow the RBAC User Creator tool to provision APIs. Do not close until you see the Success message.



Username [vsc_vmware_user] created

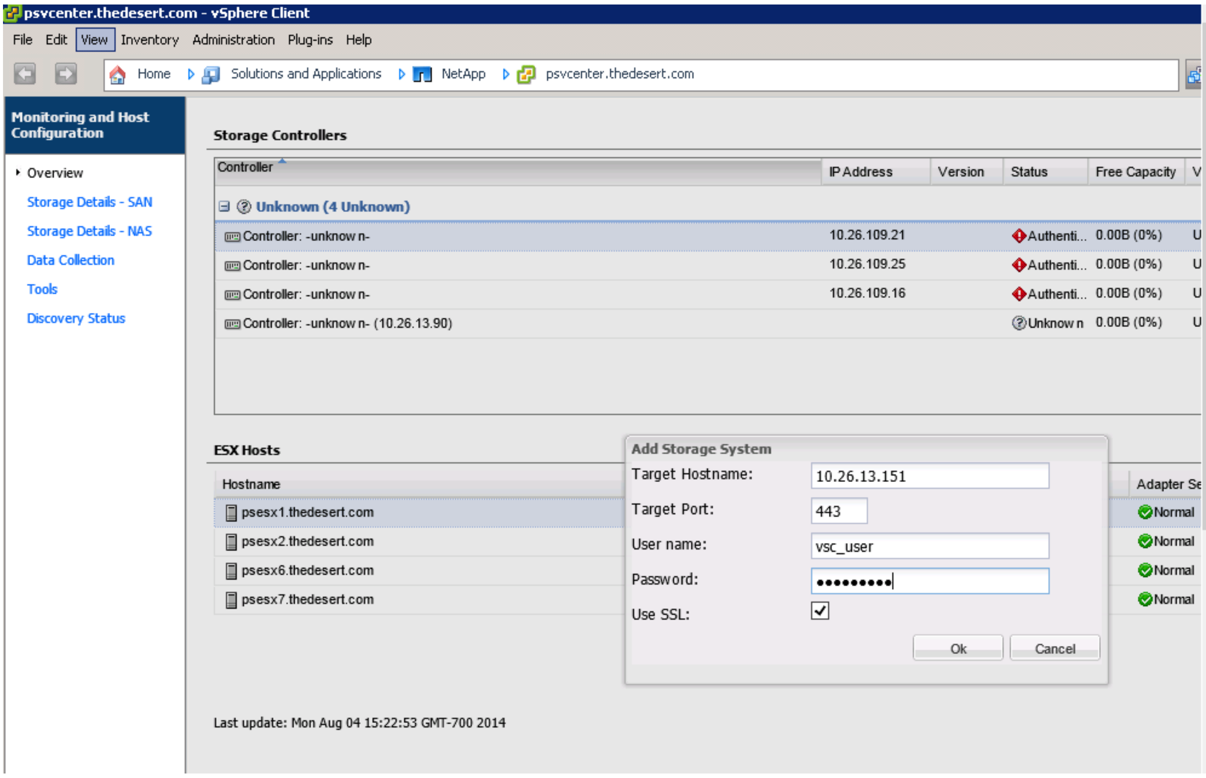
Success! - RBACUserCreator created user [vsc_vmware_user] on cluster01

4. Check at the command line interface to see if the user was created.

```
cluster01::> security login role show -role vsc_role
           Role          Command/                                      Access
Vserver    Role          Directory                               Query Level
---------- ------------- --------- ----------------------------------- --------
cluster01 vsc_role DEFAULT                                      none
cluster01 vsc_role job history show                             all
cluster01 vsc_role job show-completed                           readonly
cluster01 vsc_role lun comment                                  all
cluster01 vsc_role lun create                                   all
luster01 vsc_role lun delete                                   all
cluster01 vsc_role lun geometry                                 readonly
```

```
cluster01 vsc_role lun igroup add                               all
cluster01 vsc_role lun igroup create                            all
cluster01 vsc_role lun igroup delete                            all
cluster01 vsc_role lun igroup modify                            all
cluster01 vsc_role lun igroup new                               all
cluster01 vsc_role lun igroup set                               all
cluster01 vsc_role lun igroup show                              all
cluster01 vsc_role lun map                                      all
cluster01 vsc_role lun mapped show                              all
cluster01 vsc_role lun modify                                   all
cluster01 vsc_role lun move                                     all
cluster01 vsc_role lun new                                      all
cluster01 vsc_role lun show                                     all
20 entries were displayed.
```

5. Enter and test credentials in the vSphere VSC tool.



Storage Controllers

Controller	IP Address	Version	Status	Free Capacity	V
Unknown (4 Unknown)					
Controller: -unknow n-	10.26.109.21		Authenti...	0.00B (0%)	U
Controller: -unknow n-	10.26.109.25		Authenti...	0.00B (0%)	U
Controller: -unknow n-	10.26.109.16		Authenti...	0.00B (0%)	U
Controller: -unknow n- (10.26.13.90)			Unknow n	0.00B (0%)	U

ESX Hosts

Hostname	Adapter Se
psesx1.thedesert.com	Normal
psesx2.thedesert.com	Normal
psesx6.thedesert.com	Normal
psesx7.thedesert.com	Normal

Add Storage System

Target Hostname: 10.26.13.151

Target Port: 443

User name: vsc_user

Password: ●●●●●●●●●

Use SSL: ☑

Last update: Mon Aug 04 15:22:53 GMT-700 2014

As discussed in earlier sections, not all management tools support SVM-level credentials or all features working with SVM-level credentials. Always review the management tool “Installation and Administration Guides and Release Notes” for up-to-date guidance.

Using the RBAC User Creator tool:

- Implement the role.
- Configure your tools.
- Test the tool.
- Review the audit log after deployment to validate that everything works correctly.

8.1.2 Creating a Custom Role Using XML Files

RBAC User Creator uses an XML file called ontapPrivs.xml to define which privileges a product requires.

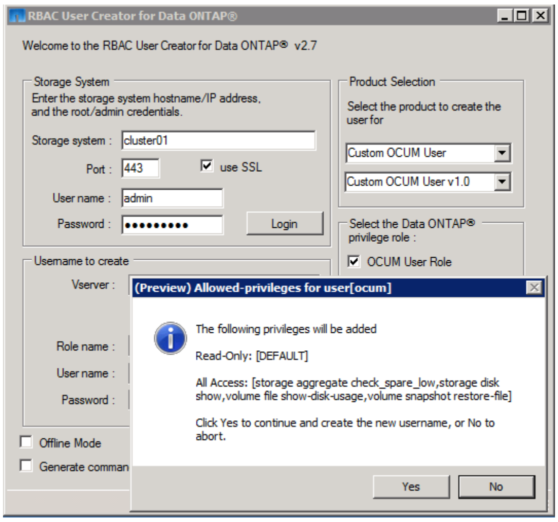
You can create privileges for custom products by adding your own XML to the ontapPrivs.xml file, before the </privs> end-tag.

In the following example we create a template for the custom OCUM role that was defined earlier in this document. You can use this template to roll out the same custom role to multiple clusters within your environment.

```
<product id="customocum" label="Custom Unified Manager User" description="">
 <customocum id="customocum10" label="Custom OCUM User v1.0">
  <cluster-mode>
   <admin-vserver>
    <role id="cOCUM" label="Unified Manager User Role" description="">
     <read-only>
      <ontap-dependent value="8.2+">
       <command>DEFAULT</command>
      </ontap-dependent>
     </read-only>
     <all-access>
      <ontap-dependent value="8.2+">
       <command>volume file show-disk-usage</command>
       <command>volume snapshot restore-file</command>
       <command>storage aggregate check_spare_low</command>
       <command>storage disk show</command>
      </ontap-dependent>
     </all-access>
    </role>
   </admin-vserver>
  </cluster-mode>
 </customocum>
</product>
```

In this example we define which release of clustered Data ONTAP this custom role can be applied to by using the <ontap-dependent value="8.2+"> tag. This information is important because releases can have variations in command syntax.

With the Custom OCUM User XML added to the ontapPrivs.xml file, you can now use the RBAC User Creator tool to create the custom role on your storage systems.



RBAC User Creator for Data ONTAP®

Welcome to the RBAC User Creator for Data ONTAP® v2.7

Storage System

Enter the storage system hostname/IP address, and the root/admin credentials.

Storage system : cluster01

Port : 443 ☑ use SSL

User name : admin

Password : ●●●●●●●●●

Product Selection

Select the product to create the user for

Custom OCUM User

Custom OCUM User v1.0

Select the Data ONTAP® privilege role :

☑ OCUM User Role

Username to create

Vserver :

Role name :

User name :

Password :

☐ Offline Mode

☐ Generate comman

(Preview) Allowed-privileges for user[ocum]

The following privileges will be added

Read-Only: [DEFAULT]

All Access: [storage aggregate check_spare_low,storage disk show,volume file show-disk-usage,volume snapshot restore-file]

Click Yes to continue and create the new username, or No to abort.

9 Summary

Role-Based Access Control changes clustered Data ONTAP to a distributed set of delegated authorities to execute discrete tasks. This change removes the risk inherent in a centralized model.

RBAC offers a secure method for efficiently managing users. Benefits of an RBAC solution include:

Increased security: User profiles and privileges can be modified rapidly. Changing policies and updating user profiles in a timely manner can help maintain high levels of security.

Security of complex organizations: RBAC provides the ability to model complex organizations through the creation of roles and the delegation of their administration. Changes can be made quickly as the organization and its security policies evolve.

Reduced complexity: Distributing administration to delegated administrators is a centralized method for managing large groups of users, thus reducing the complexity of the process.

Reduced costs: Administering authorization data is cumbersome and can create a long-term financial burden. By using delegated administrators, a company can outsource the workload to administrators within customer, supplier, and partner organizations, ultimately reducing costs.

Appendix

Resources

- RBAC Creator for Data ONTAP

  This tool is a C# application that assists you in creating RBAC user names for Data ONTAP in both 7-Mode and clustered Data ONTAP environments.
- Managing access to the cluster (8.3)
- What is clustered Data ONTAP audit information and control?
- SPI information: Clustered Data ONTAP 8.3 System Administration Guide (page 48)
- Clustered Data ONTAP 8.3 Commands: Manual Page Reference

Acronyms, Terminology

Acronyms, Terminology	Explanation
OffTap	OnCommand, all NetApp Snap products, VSC, DSM, Opens Systems SnapVault (OSSV)
Transition, Transitioning to clustered Data ONTAP	The ‘end-to-end’ process of moving Data ONTAP 7G/7-Mode and third-party environments to clustered Data ONTAP. To support, all inclusively, a successful move to clustered Data ONTAP, transition includes: • Process • Policy and technology offerings used during the assessment • Planning • Migration • Operational phases to support a successful move to clustered Data ONTAP.

Version History

Version	Date	Document Version History
Version 1.0 prerelease reviews	August 2014	First release of draft copy for review
	November 2014	Updated for clustered Data ONTAP 8.3
	January 2015	Updated per team review comments

Feedback for this document can be sent to any of its authors or posted on https://forums.netapp.com/community/acs/sx/cdot.

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.

Copyright Information

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

Trademark Information

TR-4368-0115