



Technical Report

HCI File Services Powered by ONTAP Select

Quick Start Guide

Aaron Patten, NetApp
June 2019 | TR-4669

Abstract

NetApp® ONTAP® Select extends the NetApp HCI product, adding a rich set of file and data services to the platform. This technical report details how to successfully install and configure a basic ONTAP Select HA pair for NetApp HCI using the Select Deploy appliance.

Detailed information about the advanced configuration of the ONTAP Select appliance can be found in the [ONTAP Select 9 Installation and Cluster Deployment Guide](#) and the [ONTAP Select Product Architecture and Best Practices](#) documents.

TABLE OF CONTENTS

1	Introduction	3
1.1	Software-Defined Infrastructure	3
1.2	ONTAP Feature Support	3
1.3	Use Cases	4
1.4	Prerequisites	4
2	Installing File Services Powered by ONTAP	4
2.1	Provisioning the Deploy Appliance	5
2.2	Create ONTAP Select Cluster	5
3	Configuring ONTAP Select	10
3.1	Aggregate Creation and Configuration	10
4	Create Multiprotocol File Share	11
4.1	Create SVM	12
	Conclusion	20
	Where to Find Additional Information	20
	Version History	21

1 Introduction

NetApp ONTAP Select is NetApp's solution for the software-defined storage (SDS) market. ONTAP Select brings enterprise-class storage management features to the software-defined data center. ONTAP Select extends the NetApp Data Fabric solution to the commodity server offerings likely existing in a customer's data center.

This document describes the installation process for deploying an ONTAP Select HA pair with the Select Deploy appliance. Basic configuration of the Select instance is also covered, including the creation of a single multiprotocol file share. For advanced cluster setup topics see the [ONTAP Select product documentation](#).

1.1 Software-Defined Infrastructure

The implementation and delivery of IT services through software provides administrators with the ability to rapidly provision resources with a level of speed and agility that was previously impossible.

Modern data centers are moving toward software-defined infrastructures as a mechanism to provide IT services with greater agility and efficiency. Separating IT value from the underlying physical infrastructure allows IT services to react quickly to changing IT needs by dynamically shifting infrastructure resources to where they are needed most.

Software-defined infrastructures are built on three tenets:

- Flexibility
- Scalability
- Programmability

Software-Defined Storage

The shift toward software-defined infrastructures could be having its greatest impact in an area that has traditionally been one of the least affected by the virtualization movement: storage. Software-only solutions that separate storage management services from the physical hardware are becoming more common. This fact is especially evident in private cloud environments: enterprise-class, service-oriented architectures designed from the ground up with software definition in mind. Many of these environments are built on commodity hardware: white box servers with locally attached storage and software controlling the placement and management of user data.

This approach is also seen in the emergence of hyper converged infrastructures (HCIs), a building-block style of IT design based on the premise of bundling compute, storage, and networking services. The rapid adoption of hyper converged solutions over the past several years has highlighted the desire for simplicity and flexibility. However, many companies have made the decision to replace enterprise-class storage arrays with a more customized, make-your-own model by building storage management solutions on top of homegrown components. Therefore, a new set of problems has emerged.

In a commodity world where data lives fragmented across silos of direct-attached storage, data mobility and data management have become complex problems that must be solved. NetApp can help.

1.2 ONTAP Feature Support

ONTAP Select offers full support for most ONTAP functionality except for features that have hardware-specific dependencies. Supported functionality includes the following:

- NFS, CIFS, and iSCSI
- NetApp SnapMirror® and NetApp SnapVault® technologies
- NetApp FlexClone® technology
- NetApp SnapRestore® technology

- NetApp Volume Encryption
- NetApp SnapLock® Enterprise (separate license)
- NetApp FabricPool technology (separate license)
- NetApp FlexCache® technology (separate license)
- NetApp SyncMirror® technology (separate license)
- NetApp Data Availability Services (separate license)
- NetApp MetroCluster™ SDS (formerly called an ONTAP Select two-node stretched cluster; ONTAP Select Premium license)

In addition, support for the NetApp OnCommand® management suite is included. This suite includes most tooling used to manage NetApp FAS arrays, such as OnCommand Unified Manager, OnCommand Insight, OnCommand Workflow Automation, and NetApp SnapCenter®. Using SnapCenter, NetApp SnapManager®, or NetApp SnapDrive® with ONTAP Select requires server-based licenses.

Consult the [IMT](#) for a complete list of supported management applications.

The following ONTAP features are not supported by ONTAP Select:

- Interface groups (ifgroups)
- Service Processor
- Hardware-centric features such as the traditional FAS/AFF MetroCluster architecture that requires dedicated hardware infrastructure between sites, Fibre Channel (FC and FCoE), and full disk encryption (FDE)
- NetApp Storage Encryption drives

1.3 Use Cases

The primary use cases for ONTAP Select on NetApp HCI include providing utility and departmental file services, VM template storage over NFS and home directories for mid-sized virtual desktop deployments. Replication of data in and out of cloud service providers is also supported.

1.4 Prerequisites

ONTAP Select is installed as part of a post-NDE, customer driven workflow. When you select the option to install file services powered by ONTAP, the following prerequisites must be met:

- Installation of ONTAP Select 9.5 or later
- A valid capacity license
- Pre-provisioned datastores to hold the ONTAP Select appliance VMs and their constituent storage

Note: NetApp recommends creating at least one datastore per ONTAP Select VM.

See the [ONTAP Select 9.6 Installation and Cluster Deployment Guide for VMware](#) available on the [NetApp ONTAP Select Resources page](#).

2 Installing File Services Powered by ONTAP

Installing ONTAP Select requires two primary steps:

1. Provisioning the ONTAP Deploy appliance.
2. Creating the ONTAP Select cluster with the Deploy appliance.

2.1 Provisioning the Deploy Appliance

Download the ONTAP Select Deploy utility virtual machine image from the [NetApp Support Site](#) to your local workstation. In the VMware vSphere client, select File > Deploy OVF Template. Complete the wizard specifying the appropriate values for your installation. Verify that all values are entered correctly on the final page of the wizard, and then deploy the appliance.

Deploy OVF Template

- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- ✓ 4 Review details
- ✓ 5 Select storage
- ✓ 6 Select networks
- ✓ 7 Customize template
- 8 Ready to complete**

Ready to complete
Click Finish to start creation.

Provisioning type	Deploy from template
Name	SFPS-Grimlock-Deploy
Template name	ONTAPdeploy
Download size	3.4 GB
Size on disk	5.2 GB
Folder	NetApp-HCI-Datacenter
Resource	NetApp-HCI-Cluster-01
Storage mapping	1
All disks	Datastore: NetApp-HCI-Datastore-02; Format: Thin provision
Network mapping	1
ONTAP Select Deploy VM Network	HCI_Internal_OTS_Network
IP allocation settings	
IP protocol	IPV4
IP allocation	Static - Manual

2.2 Create ONTAP Select Cluster

The following prerequisites should be in place before continuing:

- Provision one datastore for each ONTAP Select node. The minimum size should be at least 3TB each.
- Pre-provision networks for ONTAP Select management, intercluster communication, and data traffic.
- Enter vCenter and ESXi host information including credentials and IP addresses.

This example shows the deployment of a two-node, highly available cluster.

1. Log into the ONTAP Deploy appliance using the information entered in the deployment wizard. The Getting Started with ONTAP Select Deploy wizard should open automatically. Uploading licenses is optional at this stage. If no license is added, ONTAP Select VMs operate in a 90-day evaluation mode. Licenses can be added later.

ONTAP Select Deploy

Clusters Hypervisor Hosts Administration

Getting Started with ONTAP Select Deploy

Add Licenses
Add Host to Inventory
Create a Cluster
Network Precheck
Deploy the Cluster

Start by adding License file(s). Cancel Next

Click to upload licenses

Upload

License Lock ID

Licenses

Refresh

Type	Capacity	License Expiry	Serial No	Pool Name
Standard-Tier	50 TB	-		-
Standard-Tier	50 TB	-		-
Standard-Tier	50 TB	-		-
Standard-Tier	50 TB	-		-

- In the Add Host to Inventory step, select the vCenter instance to be used and then add the ESXi hosts that receive the ONTAP Select VMs during deployment.

ONTAP Select Deploy

Clusters Hypervisor Hosts Administration

✓ Host "10.193.139.145" is successfully added. ✕

Getting Started with ONTAP Select Deploy

Add Licenses
Add Host to Inventory
Create a Cluster
Network Precheck
Deploy the Cluster

Add hypervisor hosts into the Inventory. These hosts will be later used to create the clusters. Cancel Back Next

Add from a vCenter

Add

Hypervisor Host Inventory

Refresh Filtering 0 filters applied

Hypervisor Hosts	Type
✓ 10.193.139.144	ESX
✓ 10.193.139.145	ESX

- In the Create a Cluster step, enter information relevant to your deployment. In this example, a two-node HA pair is deployed. Click Done when you have entered all data.

ONTAP Select Deploy

Clusters | Hypervisor Hosts | Administration

Getting Started with ONTAP Select Deploy

Add Licenses
Add Host to Inventory
Create a Cluster
Network Precheck
Deploy the Cluster

Create a Cluster that you would like to deploy Cancel Back Next

Cluster Details

Cluster	Name sfps-grimlock-ots-cluster-01	Cluster Size 2 node cluster (1 HA Pairs)
Configuration	Host Type ESX	ONTAP Image 9.5
	Cluster MTU 9000	
Cluster Management IP	IPv4 Address 10.193.139.188	Netmask 255.255.255.0
	Gateway 10.193.139.1	
DNS Details	Domain Names rtp.openenglab.netapp.cor +	Server IP Addresses 10.193.0.250 +
	NTP Server 10.54.17.30 +	

Done

- The wizard now asks for information related to node setup for ONTAP Select. In the Nodes section, enter the node names, IP addresses, and licenses (if applicable). In the Hypervisor and Network section, select the node size; the ESXi hosts to run the Select VMs; and the networks to be used for management, cluster interconnect (internal), and data traffic.

Getting Started with ONTAP Select Deploy



Create a Cluster that you would like to deploy

Cancel Back Next

Cluster Details Edit ✎

Name	sfps-grimlock-ots-cluster-01	Cluster Size	2 node cluster (1 HA Pairs)
ONTAP Image Version	9.5	Cluster MTU	9000
Host Type	ESX	Domain Names	rtp.openenglab.netapp.com
IPv4 Address	10.193.139.188	Server IP Addresses	10.193.0.250
Netmask	255.255.255.0	NTP Server	10.54.17.30
Gateway	10.193.139.1		

Node Setup

HA Pair 1

Nodes

Node 1	Name sfps-grimlock-ots-cluster-01-C	Node Mgmt IP 10.193.139.189	Licenses 320000022 - 50 TB - Standard
Node 2	Name sfps-grimlock-ots-cluster-01-C	Node Mgmt IP 10.193.139.190	Licenses 320000023 - 50 TB - Standard

Hypervisor and Network

Instance Type: Small (4 CPU, 16 GB Memory)

Hosts: sfps-grimlock-ots-cluster-... (10.193.139.144) | sfps-grimlock-ots-cluster-... (10.193.139.145)

Management Network: HCI_Internal_OTIS_Network | Internal Network: HCI_Internal_OTIS_Cluster | Data Network: HCI_Internal_OTIS_Data

Use the above configuration for second node (sfps-grimlock-ots-cl...)

- In the Storage section of the page, select the desired storage pool capacity and the storage pool for each ONTAP Select node. Click Done when finished.

Storage

Enable Software RAID

Storage Pool Capacity: 10 TB

Storage Pool: NetApp-HCI-OTS-Cluster-01-D5-I (Capacity: 15.62 TB) | NetApp-HCI-OTS-Cluster-01-D5-I (Capacity: 15.62 TB)

⚠️ The space consumed by Select on the storage pool might be more than the storage specified with 'capacity' option because of the backend storage overhead. Ensure that adequate free space is available on the storage pool according to Storage Policy guidelines by storage pool provided

Done

- At the next screen, verify that all information for the cluster is correct, and then click Next.

Getting Started with ONTAP Select Deploy



Create a Cluster that you would like to deploy

Cancel Back Next

Cluster Details

Edit

Name	sfps-grimlock-ots-cluster-01	Cluster Size	2 node cluster (1 HA Pairs)
ONTAP Image Version	9.5	Cluster MTU	9000
Host Type	ESX	Domain Names	rtp.openenglab.netapp.com
IPv4 Address	10.193.139.188	Server IP Addresses	10.193.0.250
Netmask	255.255.255.0	NTP Server	10.54.17.30
Gateway	10.193.139.1		

Node Setup

✓ HA Pair 1

	Node 1 sfps-grimlock-ots-clus... — 10 TB	Host 1 10.193.139.144 — (Small (4 CPU, 16 GB Memory))	Edit
	Node 2 sfps-grimlock-ots-clus... — 10 TB	Host 2 10.193.139.145 — (Small (4 CPU, 16 GB Memory))	

Cancel Back Next

- In the Network Precheck step, verify all network information and then click Run to perform a network precheck. Validate that all the tests pass and then click Next.

Getting Started with ONTAP Select Deploy



Validate internal network connectivity before creating the cluster. This will avoid unexpected failures at the end.

Cancel Back Skip Next

▼ Details

Description None

Status **Pass**

Run ID 5

Host Name 10.193.139.144

Host Name 10.193.139.145

Internal Network HCI_Internal_OTS_Cluster

Internal Network HCI_Internal_OTS_Cluster

MTU 9000

vSwitch Type DistributedvSwitch

Delay 16 seconds

Mode quick

ⓘ Status

Results In Progress 0/6 Pass 6 Fail 0

Filtering 0 filters applied

The current run is complete. See the results below.

Run Again

Status	Test	Src Host	Dst Host	Start Time	End Time	Summary
✓ Pass	Setup	10.193.139.145	-	2019-02-06 08:57:28-0...	2019-02-06 08:57:40-0...	View details
✓ Pass	MTU Ping Test	10.193.139.144	10.193.139.145	2019-02-06 08:57:25-0...	2019-02-06 08:57:28-0...	View details
✓ Pass	Setup	10.193.139.144	-	2019-02-06 08:57:24-0...	2019-02-06 08:57:35-0...	View details
✓ Pass	MTU Verification Test	10.193.139.145	-	2019-02-06 08:57:23-0...	2019-02-06 08:57:24-0...	View details
✓ Pass	MTU Verification Test	10.193.139.144	-	2019-02-06 08:57:22-0...	2019-02-06 08:57:23-0...	View details

8. Specify the password for the cluster and click Create Cluster.

Getting Started with ONTAP Select Deploy



Validate internal network connectivity before creating the cluster. This will avoid unexpected failures at the end.

Cancel Back Skip Next

..... | | Cancel Create Cluster

The wizard now deploys the ONTAP Select VMs. At the completion of the wizard, log into System Manager to continue configuration of the cluster.

3 Configuring ONTAP Select

3.1 Aggregate Creation and Configuration

You must create an aggregate from the available VMDISK objects before a storage virtual machine (SVM) can be configured for file exports.

1. In OCM, select Storage > Aggregates and Disks > Aggregates. Provide a name for the aggregate, and then browse for a VMDK object to create an aggregate from. Select the “Pool 0” device for the first node and check the Mirror This Aggregate checkbox. Repeat the process to create an aggregate of the same size for the second node.

Aggregates

To create an aggregate, select a disk type then specify the number of disks.

Name:

Disk Type:

Disks of 971.99 GB each from node: sfps-grimlock-ots-cluster-01-01

The selected disk type contains the following number of non-zeroed disks: 1. If these non-zeroed disks are selected by ONTAP to create the aggregate, they will be added only after the zeroing process is complete. Note: If the system restarts during this process, the aggregate will not be created

Number of Disks: Max: 1 (excluding 0 hot spare), min: 1 for RAID0

RAID Configuration: RAID0; RAID group size of 8 disks

New Usable Capacity: 861.11 GB (Estimated)

FabricPool

Cloud Tier

[Tell me more about FabricPool](#)

Mirror this aggregate

Ensure that equal number of compatible disks (excluding hot spares) are available in the other pool (Total Used: 2 disks).

[Tell me more about mirrored aggregates](#)

There are no SSDs installed in this cluster. Install SSDs to enable Flash Pool options.

2. After creating the aggregate, you should verify that the size and available capacity are as expected and that each node has its own aggregate.

Aggregates

<input type="button" value="+ Create"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="More Actions"/> <input type="button" value="Refresh"/>							
	Status	Name	Node	Type	Used ...	Availa...	
+	✓	aggr0_sfps_grimlock_ots_clust...	sfps-grimlock-ots-cluster-01...	VMDISK	95	2.77 GB	
+	✓	aggr0_sfps_grimlock_ots_clust...	sfps-grimlock-ots-cluster-01...	VMDISK	95	2.77 GB	
+	✓	sfps_grimlock_ots_node_01_a...	sfps-grimlock-ots-cluster-01...	VMDISK	0	818.05 GB	
+	✓	sfps_grimlock_ots_node_02_a...	sfps-grimlock-ots-cluster-01...	VMDISK	0	818.05 GB	

4 Create Multiprotocol File Share

ONTAP Select supports creating multiprotocol file shares that can serve data over both NFS and SMB simultaneously. This section goes over how to quickly create a share that is accessible over NFS and SMB with the following assumptions.

- NFS access is through NFSv3, not NFSv4 or NFSv4.1.
- You want to implement best practices without reading all the relevant product documentation.

- You want to use OnCommand System Manager, not the ONTAP command-line interface or an automated scripting tool.
- You want to manage ONTAP Select through System Manager.
- Your data network uses the default IPspace, the default broadcast domain, and the default failover group.
- If your data network is flat, using these default objects makes sure that LIFs fail over correctly in the event of a link failure. If you are not using the default objects, you should refer to the [Network Management Guide](#) for information on how to configure LIF path failover.
- LDAP, if used, is provided by Active Directory.

For more complete details and restrictions, see the SMB/CIFS and NFS [multiprotocol express configuration guide](#) available on [docs.netapp.com](#).

4.1 Create SVM

You must create an SVM to facilitate file shares by completing the following steps:

1. Navigating to Storage > SVMs and selecting Create.
2. Specify the name of the SVM, the data protocols to use, the security style, the root aggregate, and the DNS information. Leave the default settings for the other fields and click Next. Select UNIX for the security style.

Storage Virtual Machine (SVM) Setup



SVM Details

? Specify a unique name and the data protocols for the SVM

SVM Name:

? IPspace: ▼

? Data Protocols: CIFS NFS iSCSI

? Default Language: ▼

The language of the SVM specifies the default language encoding setting for the SVM and its volumes. Using a setting that incorporates UTF-8 character encoding is recommended.

? Security Style: ▼

Root Aggregate: ▼

DNS Configuration

Specify the DNS domain and name servers. DNS details are required to configure the CIFS protocol.

? Search Domains:

? Name Servers:

3. In the Configure CIFS/NFS protocol window, assign an IP address and either the e0b or e0c port for the export to be served from. Additionally, provide the information required to join Active Directory. The CIFS Server Name should reflect the DNS name that you want clients to browse to on the network for CIFS shares. You must create A DNS host record for this entry if it does not already exist. Do not enter any information in the Provision a Volume for CIFS Storage (Optional) area. Doing so would provision a volume only for CIFS access, not multiprotocol access.

Storage Virtual Machine (SVM) Setup

1 Enter SVM basic details 2 **Configure CIFS/NFS protocol** 3 Enter SVM administrator details

Configure CIFS/NFS protocol

? To enable CIFS, specify the data interfaces and the CIFS server details. If you are configuring NFS, specify NIS details.
 To enable access to the NFS ports, add rules to the default export policy or create a new policy for the SVM.

Data LIF Configuration

CIFS Server Configuration

CIFS Server Name: <input type="text" value="grimlock-export"/>	Provision a volume for CIFS storage (Optional).
Active Directory: <input type="text" value="rtp.openenglab.netapp.com"/>	Share Name: <input type="text"/>
Organizational Unit: <input type="text" value="OU=Computers,OU=SFTS,DI"/>	Size: <input type="text"/> GB <input type="button" value="v"/>
Administrator Name: <input type="text" value="sftsadmin"/>	Permission: <input type="text" value="Everyone - Full Control"/> <input type="button" value="Change"/>
Administrator Password: <input type="password" value="....."/> <input type="button" value="show"/>	? <input type="checkbox"/> Encrypt data while accessing this share

? Encrypt data while accessing all the shares in this SVM

NIS Configuration (Optional)

- Expand the NIS Configuration (Optional) area and enter the details for NIS configuration if your environment uses NIS. Do not enter any information in the Provision a Volume for NFS Storage area. Doing so would provision a volume only for NFS access, not multiprotocol access. After all data has been entered, click the Submit & Continue button to continue the wizard.

Storage Virtual Machine (SVM) Setup

1 Enter SVM basic details 2 **Configure CIFS/NFS protocol** 3 Enter SVM administrator details

Configure CIFS/NFS protocol

? To enable CIFS, specify the data interfaces and the CIFS server details. If you are configuring NFS, specify NIS details.
To enable access to the NFS ports, add rules to the default export policy or create a new policy for the SVM.

▼ Data LIF Configuration

▼ CIFS Server Configuration

▲ NIS Configuration (Optional)

Configure NIS domain on the SVM to authorize NFS users.

Domain Names:

IP Addresses:

? Database Type: group passwd netgroup

Provision a volume for NFS storage.

Export Name:

Size: GB

Permission: [Change](#)

- When the SVM Administration page is displayed, you can either configure or defer configuring a separate administrator for this SVM. On the summary page click OK to finish the wizard. The SVM is now set up.

SVMs

+ Create ✎ Edit ✕ Delete ▶ Start ■ Stop 🔧 SVM Settings 🔄 Refresh					
Name	State	Subtype	Allowed Protocols		
sfps-prototype-ots-export	running	default	NFS, CIFS		

Export Policy

You must add a rule to the default export policy to allow all clients access through NFSv3. Without such a rule, all NFS clients are denied access to the SVM and its volumes. You should specify all NFS access as the default export policy, and later restrict access to individual volumes by creating custom export policies for individual volumes.

Open the SVM settings and navigate to Export Policies. Highlight the default export policy, select Add a Policy, then input the following details:

Create Export Rule [X]

Client Specification:

Rule Index: [↑] [↓]

Access Protocols: CIFS
 NFS NFSv3 NFSv4
 Flexcache

i *If you do not select any protocol, access is provided through any of the above protocols (CIFS, NFS, or FlexCache) configured on the Storage Virtual Machine (SVM).*

Access Details: Read-Only Read/Write

UNIX	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Kerberos 5	<input type="checkbox"/>	<input type="checkbox"/>
Kerberos 5i	<input type="checkbox"/>	<input type="checkbox"/>
NTLM	<input type="checkbox"/>	<input type="checkbox"/>

Allow Superuser Access
Superuser access is set to all

Create a Volume

You must now create a NetApp FlexVol® volume to contain your data.

1. Navigate to the Volumes window, click Create, and select Create FlexVol.
2. In the Create Volume window, give the volume a meaningful name, select the aggregate that you created earlier, and set the appropriate size and space reservations.

Create Volume ✕

General | Storage Efficiency | Quality of Service | Protection

Name: 📄

FabricPool: The SVM does not contain any FabricPool-enabled aggregates.
[Configure a Cloud tier.](#) [Learn more.](#)

Aggregate:

Encrypted

[Tell me more about encryption](#)

Storage Type

NAS (Used for CIFS or NFS access)

Data Protection (Used as destination volume)

Size

Total Size: ▼

Snapshot Reserve (%): ▲▼

Data Space: 475 GB

Snapshot Space: 25 GB

Space Reserve

Space Reserve (optional): ▼

[Tell me more about space reservation](#)

The volume should now be listed under the SVM.

Volumes | SVM ▼

+ Create | Edit | Delete | More Actions | View Missing Protection Relationships | Refresh

	Status	Name	Style	Aggreg...	Thin Provisi...	Availabl...	Total Sp...
+	✓	iso	FlexVol	sfps_grimloc...	No	475 GB	500 GB
+	✓	sfpsgrimlockotss...	FlexVol	sfps_grimloc...	No	972.48 MB	1 GB

- You can now edit the volume and change the security style to UNIX. For wide-open volume permissions for all UNIX user types, select all the boxes. Otherwise make selections that are appropriate for your environment. Export policies can be used to limit access to the exports.

Edit Volume

General Storage Efficiency Advanced

Name:

Security style:

Configure UNIX permissions (Optional)

	Read	Write	Execute
Owner	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Group	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Others	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Creating a Share

Before Windows users can access a volume, you must create a CIFS share on the volume.

From the Shares window, select Create Share. Specify the folder to share and the share name and then click Create.

Create Share

Folder To Share:

Share Name:

Comment:

Enable continuous availability for Hyper-V and SQL

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

Encrypt data while accessing this share

i Encrypts data using SMB 3.0 to prevent unauthorized file access on this share.

Create Export Policy

Before NFS clients can access a volume, you must create an export policy for the volume. Add a rule that permits access by an administration host, and then apply the new export policy to the volume.

1. From the SVM window, open the SVM settings and select Export Policies. Create a new policy and then under Export Rules click Add to add a new rule to the policy.

Create Export Policy

Policy Name:

Create Export Rule

Client Specification:
Enter comma-separated values for multiple client specifications

Access Protocols:

- CIFS
- NFS NFSv3 NFSv4
- Flexcache

i If you do not select any protocol, access is provided through any of the above protocols (CIFS, NFS, or FlexCache) configured on the Storage Virtual Machine (SVM).

Access Details:

Read-Only Read/Write

UNIX

Kerberos 5

Kerberos 5i

Kerberos 5p

NTLM

Allow Superuser Access
Superuser access is set to all

- In the Create Export Rule dialog box, create a rule that allows an administrator full access to the export through all protocols. The export can now be tested prior to allowing all clients to access the export. Select CIFS and NFSv3 and enable all Read/Write checkboxes. Also select Allow Superuser Access.

Policy						
ISOExportPolicy						
default						
+ Add Edit X Delete Move Up Move Down Refresh						
Rule Index	Client	Access Protocols	Read-Only Rule	Read/Write Rule	Superuser Access	
1	10.193.136.36	NFSv3, CIFS	Never	Any	Any	

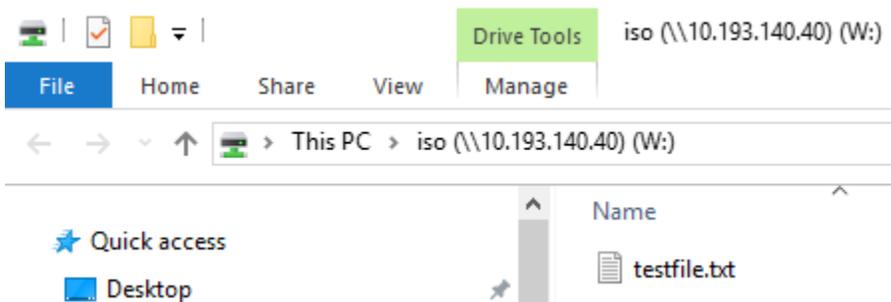
- Apply the export policy to the new volume by navigating to the Junction Path window. From here, highlight the volume and click Change Export Policy.

Junction Paths | SVM sfps-grimlock-ots-svm01 ▼

Mount Unmount Change Export Policy Refresh

Path	Storage Object	Export Policy	Security Style
/	sfpsgrimloc...	default	unix
iso	iso	ISOExportPolicy	unix

The new share should now be available and browsable by going to \\<servername>\iso on a Windows host or by mounting <servername>:/<sharepath>.



```

root@sfps-grafana-dev:~# mkdir -p /mnt/iso
root@sfps-grafana-dev:~# mount -t nfs -o nfsvers=3,hard 10.193.140.40:/iso /mnt/iso
root@sfps-grafana-dev:~# ls /mnt/iso
testfile.txt
root@sfps-grafana-dev:~# echo "written in linux!" >> /mnt/iso/testfile.txt
root@sfps-grafana-dev:~# cat /mnt/iso/testfile.txt
written in windows!!written in linux!

```

For more information about securing your fire shares and more advanced configuration of ONTAP Select, visit the [ONTAP 9 Documentation Center](#).

Conclusion

NetApp HCI is the embodiment of an API-driven, scale-out, multiworkload platform for the next-generation data center. This combination enables several key capabilities, including the following:

- Making automation and orchestration first-class citizens in the data center
- Scaling the scarcest resources without overprovisioning the entire stack
- Driving true consolidation of workloads by pushing better system utilization
- Reducing go-forward capex and opex costs
- Integrating into the NetApp Data Fabric to leverage all NetApp products, increase data mobility, and reduce data silos

Where to Find Additional Information

To learn more about the information described in this document, refer to the following documents and/or websites:

- NetApp HCI Resources
<https://mysupport.netapp.com/netapphci/resources>
- ONTAP Select Product Architecture and Best Practices
<https://fieldportal.netapp.com/content/454270>
- SMB/CIFS and NFS Multiprotocol Configuration Express Guide
https://library.netapp.com/ecm/ecm_download_file/ECMLP2495163
- ONTAP Select 9 Installation and Cluster Deployment Guide
https://library.netapp.com/ecm/ecm_download_file/ECMLP2847383

Version History

Version	Date	Document Version History
Version 1.0	March 2018	Initial release.
Version 1.1	November 2018	Update for ONTAP Select 9.4 and NetApp HCI 1.4
Version 1.2	June 2019	Update for ONTAP Select 9.5 and NetApp HCI 1.6

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

Copyright © 2019 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

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.

Data contained herein pertains to a commercial item (as defined in FAR 2.101) and is proprietary to NetApp, Inc. The U.S. Government has a non-exclusive, non-transferrable, non-sublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b).

Trademark Information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.