



Technical Report

NetApp HCI File Services Powered by ONTAP Select

Quick Start Guide

Aaron Patten, NetApp
November 2018 | 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 execute postinstallation tasks to configure an ONTAP Select instance for NetApp HCI.

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	ONTAP Select as Deployed by the NetApp Deployment Engine	4
2	Installing File Services Powered by ONTAP	6
3	Configuring ONTAP Select	6
3.1	Deploy a Network	7
3.2	Create and Configure an Aggregate	9
4	Creating a Multiprotocol File Share	10
4.1	Create a Storage Virtual Machine	11
5	Conclusion	18
	Where to Find Additional Information	19
	Version History	19

LIST OF FIGURES

Figure 1)	Volumes for ONTAP Select	5
Figure 2)	NDE Data Fabric	6
Figure 3)	Select port groups	7
Figure 4)	Broadcast domains	7
Figure 5)	Port details	8
Figure 6)	Ethernet ports	9
Figure 7)	Select management interfaces	9

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. It also extends the NetApp Data Fabric solution to the commodity server offerings that probably exist in a customer's data center.

This document describes the postinstallation configuration steps you must execute after ONTAP Select has been deployed by the NetApp Deployment Engine (NDE). 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 gives administrators 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 might 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 defined in mind. Many of these environments are being built on commodity hardware: white box servers with locally attached storage, with software controlling the placement and management of user data.

This approach is also seen in the emergence of hyper converged infrastructures, 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, as companies make 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, a new set of problems emerges.

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

1.2 ONTAP Feature Support

ONTAP Select offers full support for most of the ONTAP functionality, except for those features that have hardware-specific dependencies. The supported functionality includes:

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

- NetApp Volume Encryption (NVE)
- NetApp SnapLock® Enterprise
- FabricPool
- NetApp MetroCluster™ SDS (formerly ONTAP Select two-node stretched cluster)

Support for the NetApp OnCommand® management suite is also 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.

For a complete list of supported management applications, consult the Interoperability Matrix Tool on the NetApp Support site.

The following ONTAP features are not supported by ONTAP Select in NetApp HCI:

- iSCSI protocol
- Interface groups (ifgroups)
- Service processor
- Hardware-centric features such as the traditional FAS/AFF MetroCluster architecture, which requires dedicated hardware infrastructure between sites, Fibre Channel (FC/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 midsized virtual desktop deployments. ONTAP Select, as deployed by NDE, is not positioned as a primary storage platform for virtual machines hosted on NetApp HCI.

1.4 ONTAP Select as Deployed by the NetApp Deployment Engine

When you select the option to install file services powered by ONTAP, the following are prerequisites:

- Installation of ONTAP Select 9.3 or later
- A valid capacity license; evaluation licenses are not supported
- Provisioning of at least two NetApp SolidFire® volumes
 - One 537GB volume for the ONTAP Select VM root file system
 - One 3.1TB volume for every 2TB of licensed capacity for data storage (Figure 1 shows an 8TB configuration.)

Figure 1) Volumes for ONTAP Select.

Name	Account	Access Groups	Access	Used	Size
NetApp-HCI-Select-Data-04	NetApp-HCI	NetApp-HCI	Read / Write	0.00%	3.1 TB
NetApp-HCI-Select-Data-03	NetApp-HCI	NetApp-HCI	Read / Write	0.00%	3.1 TB
NetApp-HCI-Select-Data-02	NetApp-HCI	NetApp-HCI	Read / Write	0.00%	3.1 TB
NetApp-HCI-Select-Data-01	NetApp-HCI	NetApp-HCI	Read / Write	0.00%	3.1 TB
NetApp-HCI-Select-Install	NetApp-HCI	NetApp-HCI	Read / Write	2.53%	536.9 GB

By default, the quality of service (QoS) for all ONTAP Select volumes is set to the default 50/15000; that is, 15000 for minimum, maximum and burst IOPS respectively. For higher performance file shares, these values might need to be increased.

The following restrictions are in place for OTS deployments through NDE:

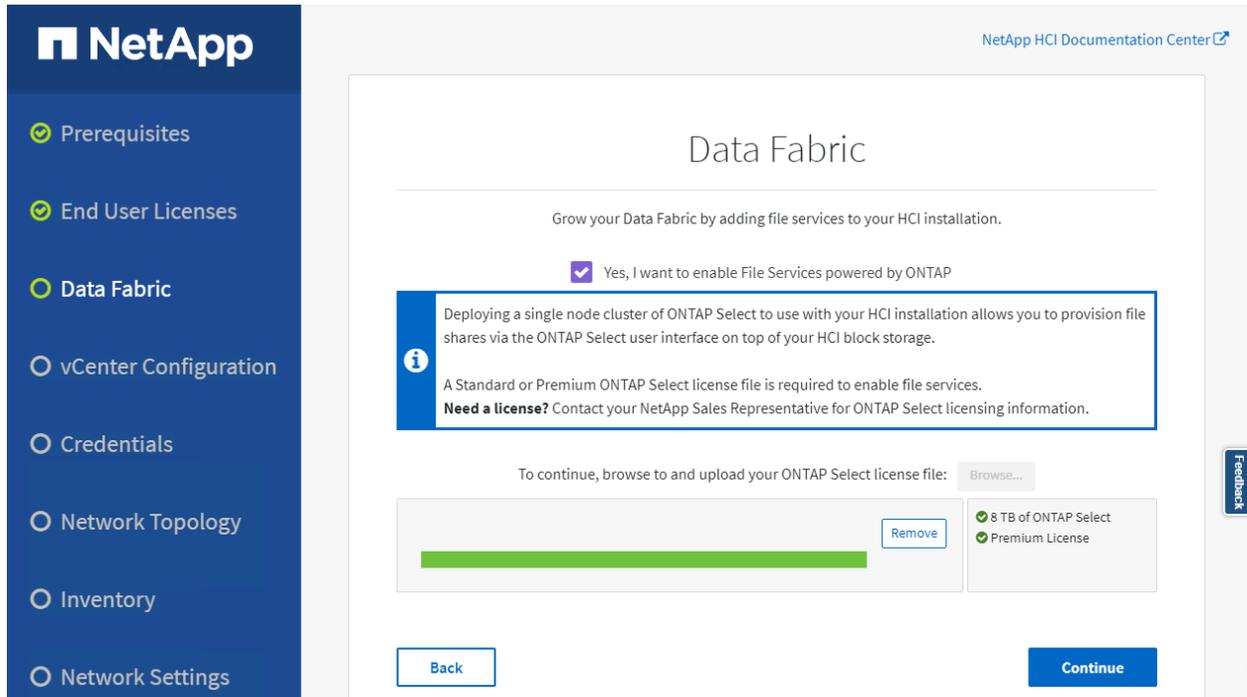
- The iSCSI protocol license is removed
- 8TB is the maximum license capacity
- Single-node deployments only – no ONTAP Select HA

For full-featured, multimode deployments with more than 8TB of capacity, ONTAP Select should be deployed through the Select Deploy appliance instead of through NDE. See the ONTAP Select 9.4 Installation and Cluster Deployment Guide for VMware on the NetApp ONTAP Select Resources page: <https://www.netapp.com/us/documentation/ontap-select.aspx>.

2 Installing File Services Powered by ONTAP

File Services powered by ONTAP is an optional component in NDE. To enable it, select the “Yes, I want to enable File Services powered by ONTAP” option in the Data Fabric section of the NDE. Selecting this option deploys a single, non-HA, ONTAP Select VM.

Figure 2) NDE Data Fabric.



Note: If a highly available ONTAP Select deployment is desired, the ONTAP Select Deploy appliance must be used to deploy ONTAP Select instead of NDE. Refer to the [ONTAP Select 9 Installation and Cluster Deployment Guide for VMware](#) for more information.

When you enable file services, you are required to provide a valid capacity license file before continuing. The NDE handles provisioning of the ONTAP Select VM by automating the following tasks:

- Installation of a single ONTAP Select appliance
- Application of the license file
- Application of the node and cluster management IPs
- Provision capacity to the ONTAP Select VM for file services

After the system is deployed, the ONTAP Select VM requires execution of some postconfiguration tasks.

3 Configuring ONTAP Select

You might need to execute several postconfiguration tasks to provide file services from the ONTAP Select VM. These tasks include:

- Modifying the network adapter configuration, if required
- Creating one or more aggregates
- Creating one or more storage virtual machines (SVMs)
- Configuring desired file services (NFS, SMB, and so on)

- (Optional) Configuring other services, such as SnapMirror

3.1 Deploy a Network

The ONTAP Select appliance is deployed with three network adapters. By default, all three network adapters for the Select VM are connected to the HCI_Internal_OTS_Network port. NetApp recommends moving network adapters 2 and 3 to a port group backed by 10Gb interfaces. This new port group might have to be created, depending on your desired configuration.

Figure 3) Select port groups.

> Network adapter 1	HCI_Internal_OTS_Network ▾
> Network adapter 2	VM_Network ▾
> Network adapter 3	VM_Network ▾

When viewing the adapters through OnCommand System Manager, all network adapters are bound to the default IPspace and broadcast domain. Before making any further configuration changes, you should move ports e0b and e0c to a dedicated broadcast domain for serving data.

Figure 4) Broadcast domains.

Create Broadcast Domain

Specify the broadcast domain details and assign ports to it.

Name:

MTU:

IPspace: ▾

Assign Ports: Ports that can be assigned to a new broadcast domain are shown below.

	Port Name	ontap-select-node
<input checked="" type="checkbox"/>	e0b	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	e0c	<input checked="" type="checkbox"/>

If you're using a 10Gb network for data connections to ONTAP Select, you might also need to change the ethernet port speed and MTU to match the target network configuration.

Figure 5) Port details.

The screenshot shows a dialog box titled "Edit Ethernet Port" with a close button (X) in the top right corner. The dialog is divided into several sections:

- Port Information:** A table-like structure showing:
 - IPspace: Default
 - Port: e0b
 - Broadcast Domain: -NA-
 - Status: Enabled
 - Node: ontap-select-node
 - Type: physical
- MTU Size (in Bytes):** A text input field containing "9000" with up and down arrow buttons.
- Duplex Mode and Speed:** A section with two radio buttons:
 - Auto Negotiate: Automatically determines the duplex mode and the highest speed that the port and its end point can support.
 - Manual Settings: Specify the duplex mode and speed that you prefer the port to use. Depending on network limitations, actual setting might be lower than the specified setting.
- Duplex Mode:** A dropdown menu currently set to "full".
- Speed:** A dropdown menu currently set to "10000 Mbps".
- Buttons:** "Save" and "Cancel" buttons at the bottom.

Figure 6) Ethernet ports.

Ethernet Ports

+ Create Interface Group + Create VLAN Edit X Delete Refresh

Port	Node	Broadcast Domain	IPspace	Type	Administrative Status
e0a	ontap-select-node	Default	Default	physical	↑
e0b	ontap-select-node	Data-VLAN101	Default	physical	↑
e0c	ontap-select-node	Data-VLAN101	Default	physical	↑

Ethernet Port Properties

Administrative		Operational	
Auto Negotiation:	false	Auto Negotiation:	false
Duplex Mode:	full	Duplex Mode:	full
Speed:	1000	Speed:	
MTU Size (in Bytes):	1500	Health Status:	✔ Healthy

Interfaces on the Port

Interface Name	SVM	IP Address
cluster_mgmt	ontap-select-clus...	10.193.139.35
ontap-select-nod...	ontap-select-clus...	10.193.139.36

The cluster and node management interfaces are defined on port e0a. Ports e0b and e0c are available for hosting data LIFs for customer traffic.

Figure 7) Select management interfaces.

Interfaces on the Port

Interface Name	SVM	IP Address	At Home
cluster_mgmt	ontap-select-cluster	10.193.139.35	true
ontap-select-node_mgmt1	ontap-select-cluster	10.193.139.36	true

3.2 Create and Configure an Aggregate

You must create an aggregate from the available VMDISK objects before an SVM can be configured for file exports.

1. In OnCommand System Manager under Storage > Aggregates and Disks > Aggregates, add all the available VMDISKS to a new aggregate.

Aggregates: Create Aggregate

Enter Aggregate Details

Manually Create Aggregate

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

Name:

Disk Type:

Disks of 1.88 TB each from node: ontap-select-node

Number of Disks: Max: 4 (excluding 0 hot spare), min: 1 for RAID0

RAID Configuration: RAID0; RAID group size of 8 disks

New Usable Capacity: 6.65 TB (Estimated)

FabricPool

[Tell me more about FabricPool](#)

Mirror this aggregate

[Tell me more about mirrored aggregates](#)

- After creating the aggregate, you should verify that the size and available capacity were set up correctly.

Aggregates

	Status	Name	Node	Type	Used ...	Availa...	Used ...	Total ...
<input type="checkbox"/>	✓	aggr_hci_01	ontap-sel...	VMDISK	0	6.65 TB	232 KB	6.65 TB
<input type="checkbox"/>	✓	aggr0_ont...	ontap-sel...	VMDISK	95	3.01 GB	58.98 GB	61.99 GB

4 Creating a Multiprotocol File Share

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

- NFS access will be 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 ensures that LIFs will fail over correctly in the event of a link failure. If you are not using the default objects, refer to the Network Management Guide for information about how to configure LIF path failover.
- LDAP, if used, is provided by Active Directory.

For complete details and restrictions, refer to the [SMB/CIFS and NFS Multiprotocol Configuration Express Guide](#).

4.1 Create a Storage Virtual Machine

1. You must create a storage virtual machine (SVM) to facilitate file shares. To create an SVM, navigate to Storage > SVMs and select Create.
2. In SVM details, specify the name of the SVM, data protocols to use, security style, root aggregate, and DNS information. Retain the default settings of the other fields and click Next. Select UNIX for the security style.

Storage Virtual Machine (SVM) Setup

● — 1 — ●
Enter SVM basic details

SVM Details

Specify a unique name and the data protocols for the SVM

SVM Name:

IPspace:

Data Protocols: CIFS NFS NVMe

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. Also provide the information required to join Active Directory.

Note: 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.

4. Do not enter any information in the Provision a Volume for CIFS Storage (Optional) area. This would provision a volume only for CIFS access, not for multiprotocol access.

The screenshot shows the 'Storage Virtual Machine (SVM) Setup' wizard. At the top, a progress bar indicates three steps: 1. Enter SVM basic details, 2. Configure CIFS/NFS protocol (current step), and 3. Enter SVM administrator details. The main heading is 'Configure CIFS/NFS protocol'. Below this, there is a help icon and text: '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.' There are two expandable sections: 'Data LIF Configuration' and 'CIFS Server Configuration'. Under 'Data LIF Configuration', there is a checked checkbox 'Retain the CIFS data LIF's configuration for NFS clients.' Below this, 'Data Interface details for CIFS' includes 'Assign IP Address:' with a dropdown set to 'Without a subnet' and an IP address of '10.193.140.40' with a 'Change' link. The 'Port:' is set to 'ontap-select-node:e0b' with a 'Browse...' button. Under 'CIFS Server Configuration', there are fields for 'CIFS Server Name' (hci-export), 'Active Directory' (rtp.openenglab.netapp.com), 'Organizational Unit' (OU=Computers,OU=SFTS,DI...), 'Administrator Name' (sftsadmin), and 'Administrator Password' (masked). To the right of these fields is the 'Provision a volume for CIFS storage (Optional)' section, which includes 'Share Name:', 'Size:' (with a 'GB' dropdown), and 'Permission:' (Everyone - Full Control with a 'Change' link). At the bottom, there are two checkboxes: 'Encrypt data while accessing all the shares in this SVM' and 'Encrypt data while accessing this share', both currently unchecked.

5. If your environment uses NIS, expand the NIS Configuration (Optional) area and enter the details for NIS configuration. Do not enter any information in the Provision a Volume for NFS Storage area. This would provision a volume only for NFS access, not for multiprotocol access.
6. When all the data has been entered, click the Submit and 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		

Add a Rule to the 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 storage virtual machine 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 details shown in the following screenshot.

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 FlexVol Volume

You must now create a FlexVol® volume to contain your data. Navigate to the Volumes window, click Create, and select Create FlexVol.

1. 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:

Aggregate:

Storage Type

NAS (Used for CIFS or NFS access)

Data Protection (Used as destination volume)

Tiering Policy

Policy: ▼

[Tell me more about external capacity tier and tiering policies.](#)

Size

Total Size: ▼

Snapshot Reserve (%): ▼

Data Space: 475 GB

Snapshot Space: 25 GB

Space Reserve

Space Reserve (optional): ▼

2. The volume should now be listed under the SVM.

Volumes on SVM ▼

	Status	Name	Style	Aggre...	Thin ...	Availa...	Total Space
<input type="checkbox"/>	✓	iso	FlexVol	aggr_hci_01	No	475 GB	500 GB
<input type="checkbox"/>	✓	sfpsprotot...	FlexVol	aggr_hci_01	No	972.54 MB	1 GB

3. 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. You can use export policies 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"/>

Create a Share

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

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

Create Share

Folder To Share:

Share Name:

Comment:

Enable continuous availability for Hyper-V and SQL

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

Encrypt data while accessing this share

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

Create an 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. In 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.

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

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

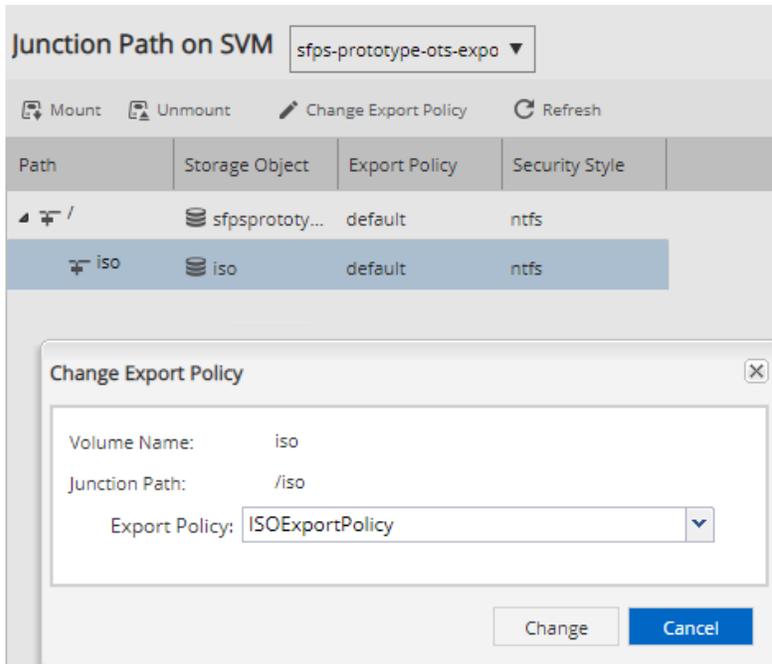
i If you do not select any protocol, access is provided through any of the above protocols (CIFS, NFS, or FlexCache) configured on the Storage Virtual Machine (SVM).

Access Details:

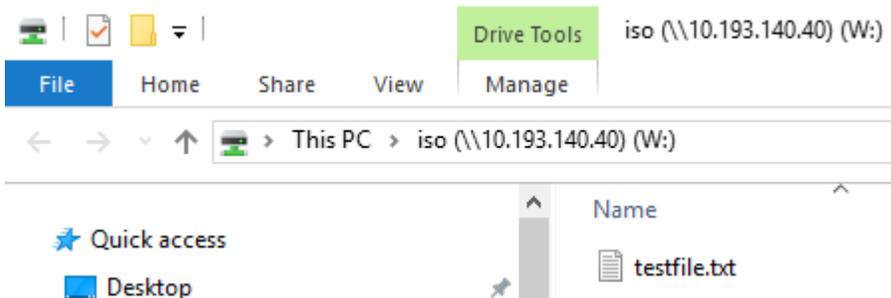
	<input type="checkbox"/> Read-Only	<input checked="" type="checkbox"/> Read/Write
<hr/>		
UNIX	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Kerberos 5	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Kerberos 5i	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Kerberos 5p	<input type="checkbox"/>	<input checked="" type="checkbox"/>
NTLM	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Allow Superuser Access		
<small>Superuser access is set to all</small>		

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	

- Now apply the export policy to the new volume. Navigate to the Junction Path on SVM window, highlight the volume, and click Change Export Policy.



- The new share should now be available and browsable. To access it, go to [\\<servername>/iso](https://<servername>/iso) on a Windows host or mount `<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, go to the [ONTAP 9 Documentation Center](#).

5 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:

- 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 capex and opex costs going forward
- 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

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 © 2018 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.