

**Multi-Protocol on cDOT**

**Authors:** Ian Daniel

**Contributors:**  Craig Goettig

**Document Version:** V0.5

**Date:** August 2017

Status: Draft

**CONFIDENTIAL INFORMATION**

This document contains information proprietary to Thomson Reuters and may not be reproduced, disclosed or used in whole or part without express permission of Thomson Reuters.

© Thomson Reuters 2017

Contents

[1 Introduction 4](#_Toc447102654)

[1.1 Management Summary 4](#_Toc447102655)

[1.2 Change History 4](#_Toc447102656)

[1.3 Distribution List 5](#_Toc447102657)

[1.4 Glossary 5](#_Toc447102658)

[2 Multi-Protocol Configuration 6](#_Toc447102659)

[2.1 Pre-requisites 6](#_Toc447102660)

[2.2 Vserver and LIF creation 6](#_Toc447102661)

[2.2.1 Create Vserver (replace hyphen with underscore in vserver rootvolume name) 6](#_Toc447102662)

[2.2.2 Create LIF with default route and failover group 6](#_Toc447102663)

[2.3 Volume creation 7](#_Toc447102664)

[2.3.1 Create Volume 7](#_Toc447102665)

[2.3.2 Set Volume Permissions to 777 7](#_Toc447102666)

[2.3.3 Create export policies (repeat this step for each volume) 7](#_Toc447102667)

[2.3.4 Create the default export-policy rule (repeat this command for every nfs client) 7](#_Toc447102668)

[2.3.5 Create volume export policy rule (repeat this command for each volume and nfs client) 7](#_Toc447102669)

[2.4 Qtree Creation 7](#_Toc447102670)

[2.4.1 Create Qtree 7](#_Toc447102671)

[2.4.2 Create Quota 7](#_Toc447102672)

[2.4.3 Apply Quota 7](#_Toc447102673)

[2.4.4 Set Qtree UNIX Permissions to 777 7](#_Toc447102674)

[2.5 Primary job schedule and snapshot policy configuration 8](#_Toc447102675)

[2.5.1 Create job schedule and snapshot policy: 8](#_Toc447102676)

[2.5.2 Setup snap autodelete on volumes (run for each SNAP volume) 8](#_Toc447102677)

[2.6 Add volumes to export & snapshot policies 8](#_Toc447102678)

[2.7 DNS configuration 8](#_Toc447102679)

[2.7.1 Setup DNS on a Vserver 8](#_Toc447102680)

[2.8 Showmount script user 8](#_Toc447102681)

[2.9 Create CIFS Server 8](#_Toc447102682)

[2.10 CIFS Share Creation 9](#_Toc447102683)

[2.10.1 Create Share 9](#_Toc447102684)

[2.11 Default User Mapping 9](#_Toc447102685)

[2.11.1 Create Default UNIX User Account and Group For Default Mapping 9](#_Toc447102686)

[2.11.2 Create Default CIFS Default User Mapping 9](#_Toc447102687)

[2.11.3 Create Default NFS Default User Mapping 9](#_Toc447102688)

[2.12 User Mapping Rules 9](#_Toc447102689)

[2.12.1 Create User Account and Group For Mapping 9](#_Toc447102690)

[2.12.2 Create CIFS User Mapping Rules 9](#_Toc447102691)

[2.12.3 Create NFS User Mapping Rules 9](#_Toc447102692)

[2.13 QoS policy group creation 10](#_Toc447102693)

[2.13.1 Create QoS policy group per volume and apply 10](#_Toc447102694)

[2.14 Cluster and Vserver Peering 10](#_Toc447102695)

[2.14.1 Confirm that cluster peering has been enabled 10](#_Toc447102696)

[2.14.2 Create the cluster peer (skip this step if cluster peering has been configured) 10](#_Toc447102697)

[2.14.3 Confirm if vserver peering has been configured 10](#_Toc447102698)

[2.14.4 Create vserver peering on the destination system (skip this step if vserver peering has been configured) 10](#_Toc447102699)

[2.14.5 Accept the vserver peering on the source system 10](#_Toc447102700)

[2.15 SnapVault configuration 10](#_Toc447102701)

[2.15.1 Create secondary volumes for SnapVault as type “DP” on the destination cluster 10](#_Toc447102702)

[2.15.2 Create a cron job schedule if it does not exist in the destination 10](#_Toc447102703)

[2.15.3 Configure a snapmirror policy on the destination 11](#_Toc447102704)

[2.15.1 Initialize SnapVault relationship on the destination 11](#_Toc447102705)

[3 Diagnosing Multi-Protocol Issues 12](#_Toc447102706)

[3.1 User Mapping 12](#_Toc447102707)

[3.1.1 Check AD name resolution: 12](#_Toc447102708)

[3.1.2 Check Unix name resolution: 12](#_Toc447102709)

[3.1.3 Check Windows to Unix mapping: 12](#_Toc447102710)

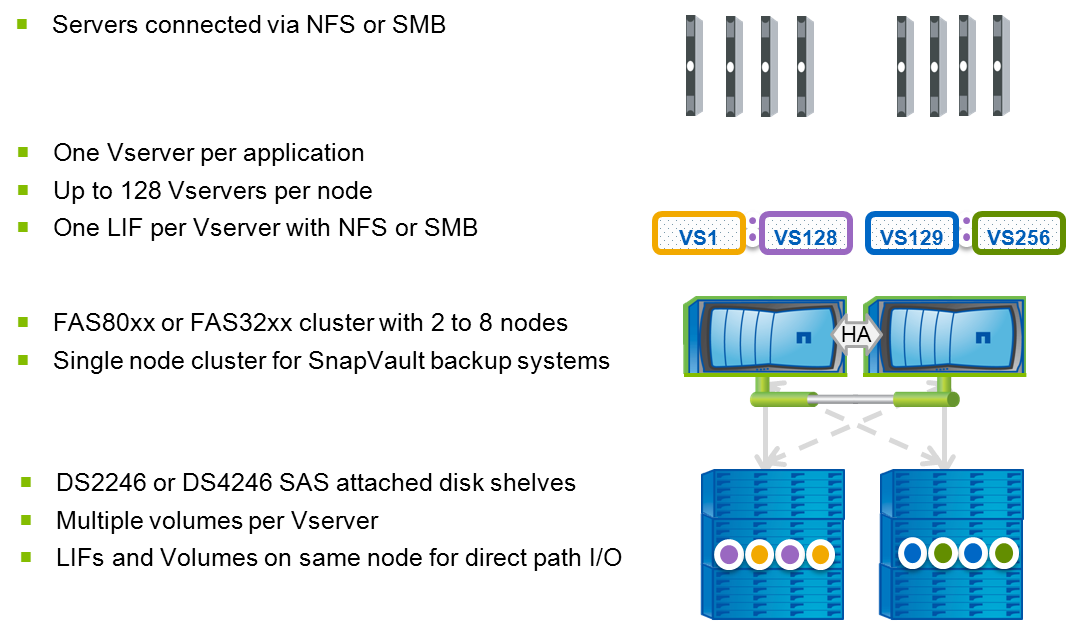
[3.1.4 Check Windows to Unix mapping: 12](#_Toc447102711)

# Introduction

## Management Summary

This document details the process used to configure multi-protocol access in cDOT. At this time the solution mirrors the current standards used for 7-Mode.

The diagram below shows an overview of the current cDOT architecture.



## Change History

|  |  |  |  |
| --- | --- | --- | --- |
| **Ver** | **Date** | **Author** | **Key Changes** |
| 0.1 | February 2016 | Ian Daniel | Initial Version |
| 0.2 | March 2016 | Ian Daniel | Added section on mapping users |
| 0.3 | March 2016 | Ian Daniel | Fixed typo |
| 0.4 | March 2016 | Ian Daniel | Added diagnostic commands |
| 0.5 | August 2017 | Ian Daniel | Modified default export policy |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## Distribution List

|  |  |
| --- | --- |
| **Name** | **Role** |
| Storage Engineering | Reviewer |
| Storage Delivery | Reviewer |
| Storage Architecture | Reviewer |

## Glossary

|  |  |
| --- | --- |
| **Term** | **Definition** |
| cDOT | clustered Data ONTAP |
| Vserver | A logical storage virtual server, also known as a Storage Virtual Machine (SVM), which contains LIFs, Volumes, and configuration information such as access control details. |
| LIF | Logical Interface – a cDOT logical network interface with an IP address, assigned to a single Vserver. |
| CIFS | Short for Common Internet File System, a protocol that defines a standard for remote file access using millions of computers at a time. With CIFS, users with different platforms and computers can share files without having to install new software. |
| SMB | Short for Server Message Block, a message format used by DOS and Windows to share files, directories and devices. |
| NFS | A distributed file system protocol originally developed by Sun Microsystems in 1984, allowing a user on a client computer to access files over a computer network much like local storage is accessed. |

# Multi-Protocol Configuration

## Pre-requisites

* Confirm the target aggregate has sufficient capacity
* Confirm the target cluster has an NFS license
* Confirm the target cluster has an CIFS license
* Confirm there is network connectivity between the client and the cluster.
* Make a note of the required CIFS Domain.
* Make a note of required DNS servers.
* Ensure you have an account with permissions to add the vserver to the required domain.
* Ensure that the cDOT AV solution is available and active for the cluster you are creating a multi-protocol vserver on.

## ****Vserver and LIF creation****

### Create Vserver (replace hyphen with underscore in vserver rootvolume name)

vserver create -vserver <vsname> -rootvolume <vsname>\_root -aggregate <aggrname> -ns-switch file -nm-switch file -rootvolume-security-style unix -language <language>

vserver show

**Note:** vserver language is inherited by volumes and should be set to en\_US

### Create LIF with default route and failover group

network interface create -vserver <vsname> -lif <vsname>-lif-<lif#> -role data -data-protocol nfs,cifs -home-node <node> -home-port <port> -address <ip> -netmask <netmask> -status-admin up -firewall-policy mgmt -failover-group <group>

network routing-groups route create -vserver <vsname> -routing-group d<network>/<mask> -destination 0.0.0.0/0 -gateway <gateway>

vserver show

network interface show

network interface show -failover

network routing-groups route show –vserver <vsname>

## ****Volume creation****

### Create Volume

volume create -vserver <vserver> -volume <volume\_name> -aggregate <aggregate\_name> -size <size\_of\_volume> -junction-path /<volume\_name>

volume mount -vserver <vserver> -volume <volume\_name> -junction-path /<volume\_name>

volume show -vserver <vserver> -junction

### Set Volume Permissions to 777

vol modify -vserver <vserver> -volume <volume\_name> -unix-permissions 777

### Create export policies (repeat this step for each volume)

vserver export-policy create –vserver <vsname> –policyname <volume\_name>

### Create the default export-policy rule (repeat this command for every nfs client)

vserver export-policy rule create -vserver <vsname> -policyname default -clientmatch <nfsclient> -rorule sys -rwrule never -superuser never

### Create volume export policy rule (repeat this command for each volume and nfs client)

vserver export-policy rule create -vserver <vsname> -policyname <volume\_name> -clientmatch <nfsclient> -rorule sys -rwrule sys -superuser sys -protocol nfs3

## ****Qtree Creation****

### ****Create Qtree****

volume qtree create -vserver <vsname> -volume <volume\_name> -qtree <qtree> -security-style unix

### ****Create Quota****

volume quota policy rule create -vserver <vsname> -policy-name default -volume <volume\_name> -type tree -target <qtree> -disk-limit <quota\_limit>

### ****Apply Quota****

volume quota on -vserver <vsname> -volume <volume\_name>

### ****Set Qtree UNIX Permissions to 777****

qtree modify -vserver <vsname> -volume <volume\_name> -qtree <qtree> -unix-permissions 777

## ****Primary job schedule and snapshot policy configuration****

### Create job schedule and snapshot policy:

job schedule cron create -name <volume\_name> -minute <min> -hour <hour>

volume snapshot policy create -vserver <vsname> -policy <volume\_name> -enabled true -schedule1 <volume\_name> -count1 7 -snapmirror-label1 snapvault -prefix1 sv\_<volume\_name>

job schedule cron show -name <vol\_name>

volume snapshot policy show –vserver <vsname>

### Setup snap autodelete on volumes (run for each SNAP volume)

volume modify -vserver <vsname> -volume <volname> -space-mgmt-try-first snap\_delete

volume snapshot autodelete modify -vserver <vsname> -volume <vol\_name> -enabled true

volume snapshot autodelete modify -vserver <vsname> -volume <vol\_name> -trigger snap\_reserve

volume show -vserver <vsname> -fields space-mgmt-try-first

volume snapshot autodelete show -vserver <vsname>

## Add volumes to export & snapshot policies

volume modify -volume <volume\_name> -policy <volume\_name> -snapshot-policy <volume\_name> -vserver <vserver>

## ****DNS configuration****

### Setup DNS on a Vserver

vserver services dns create -vserver <vsname> -domains <domainname> -name-servers <comma\_separate\_name\_server\_list>

vserver services dns show

## Showmount script user

security login role create -role showmount -cmddirname "vserver export-policy" -access readonly -vserver <vserver>

security login role create -role showmount -cmddirname volume -access readonly -vserver <vserver>

security login role create -role showmount -cmddirname "version" -access all -vserver <vsname>

security login create -username shwmnt -application ontapi -authmethod password -role showmount -vserver <vserver>

## ****Create CIFS Server****

cifs server create -vserver <vsname> -cifs-server <vsname> -domain -ou ou=<OU>,ou=<OU>,ou=<OU>

## ****CIFS Share Creation****

### ****Create Share****

cifs share create -share-name <share\_name> -path <Path\_To\_Data> -vserver <vsname>

## ****Default User Mapping****

User mapping can be used in two different ways to enable file permissions to be set as required. These consist of either setting a single default user/group for UNIX🡪Windows and Windows🡪UNIX or the addition of mapping rules and UNIX users to facilitate a more detailed level of user mapping. The UID and GID used on the vserver must correspond to the user on the UNIX server.

### ****Create Default UNIX User Account and Group For Default Mapping****

unix-user create -vserver si-8040-test-02 -user <UNIX\_User> -id <UID> -primary-gid <GID>

unix-group create -vserver si-8040-test-02 -name helpdesk -id <GID>

### ****Create Default CIFS Default User Mapping****

cifs options modify -vserver <vsname> -default-unix-user <UNIX\_User>

### ****Create Default NFS Default User Mapping****

vserver nfs modify -vserver <vsname> -default-win-user <DOMAIN\\Username>

## ****User Mapping Rules****

With the addition of mapping rules and UNIX users we can facilitate a more detailed level of user mapping as opposed to the 1-1 mapping you get by just setting default users. By default a users domain login will map to a UNIX login that matches i.e. ten\uc123456 will map to uc123456. There must be a matching UNIX user setup on the cDOT vserver for this to work.The UID and GID used on the vserver must correspond to the user on the UNIX server.

### ****Create User Account and Group For Mapping****

unix-user create -vserver <vsname> -user <UNIX\_User> -id <UID> -primary-gid <GID>

unix-group create -vserver <vsname> -name helpdesk -id <GID>

### ****Create CIFS User Mapping Rules****

This rule will match any TEN domain user and map the user portion to a UNIX user configured on the vserver i.e. TEN\uc123456 🡪 c123456 (note it is NOT case sensitive)

vserver name-mapping create -vserver <vsname> -direction win-unix -position 2 -pattern ten\\(.)(.+) -replacement \2

### ****Create NFS User Mapping Rules****

This rule will match any UNIX user configured on the vserver and map the user portion to a CIFS TEN user i.e. c123456 🡪 TEN\uc123456

vserver name-mapping create -vserver <vsname> -direction unix-win -position 1 -pattern (.+) -replacement TEN\\\u\1

## ****QoS policy group creation****

### Create QoS policy group per volume and apply

qos policy-group create -policy-group <volname> -vserver <vsname> -max-throughput 6000iops

volume modify -vserver <vsname> -volume <volume> -qos-policy-group <volname>

qos policy-group show

volume show –vserver <vsname> -fields qos-policy-groupSnapvault Configuration

## Cluster and Vserver Peering

### Confirm that cluster peering has been enabled

cluster peer show

### Create the cluster peer (skip this step if cluster peering has been configured)

cluster peer create -peer-addrs <remote\_ICL\_IP1,remote\_ICL\_IP2> -username admin

cluster peer show

### Confirm if vserver peering has been configured

vserver peer show

### Create vserver peering on the destination system (skip this step if vserver peering has been configured)

vserver peer create -vserver <destination\_vserver> -peer-cluster <source\_cluster> -peer-vserver <source\_vserver> -applications snapmirror

vserver peer show

### Accept the vserver peering on the source system

vserver peer accept -vserver <source\_vserver> -peer-vserver <destination\_vserver>

vserver peer show

## SnapVault configuration

### Create secondary volumes for SnapVault as type “DP” on the destination cluster

volume create -vserver <vserver> -volume <volume\_name> -aggregate <aggr\_name> -size <size> -security-style unix -space-guarantee none -percent-snapshot-space 0 -language <vol\_language> -type DP

volume show

### Create a cron job schedule if it does not exist in the destination

job schedule cron create -name xdp\_<hour> -minute 00 -hour <hour>

job schedule show

### Configure a snapmirror policy on the destination

* **7 day retention will have a snapshot count of 7 on the secondary**
* **14 day retention will have a snapshot count of 14 on the secondary**
* **30 day retention will have a snapshot count of 30 on the secondary**
* **45 day retention will have a snapshot count of 45 on the secondary**

snapmirror policy create -vserver <vserver> -policy <volume>

snapmirror policy add-rule -vserver <vserver> -policy <volume> -snapmirror-label snapvault -keep <retention#>

snapmirror show -destination-path \* -fields Schedule

snapmirror policy show

### Initialize SnapVault relationship on the destination

snapmirror create -source-path <source\_vserver>:<source\_volume> -destination-path <destination\_vserver>:<destination\_volume> -type XDP -schedule <schedule\_name> -policy <policy\_name>

snapmirror initialize -destination-path <destination\_vserver>:<destination\_volume>

snapmirror show

# Diagnosing Multi-Protocol Issues

There are a number of useful commands for diagnosing issues with Multiprotocol shares, the main ones are summarized below. You need to be at diag privilege for these commands to be available.

## User Mapping

### Check AD name resolution:

diag secd authentication translate –node <node> -vserver <vserver> -win-name <username>

**Example**

eg-si-clsn-e01::\*> diag secd authentication translate -node eg-si-clsn-e01-h01 -vserver si-8040-test-02 -win-name ten\uc136758

S-1-5-21-2012327785-2259879848-3711903672-181740

### Check Unix name resolution:

diag secd authentication translate –node <node> -vserver <vserver> -unix-user-name <username>

**Example**

eg-si-clsn-e01::\*> diag secd authentication translate -node eg-si-clsn-e01-h01 -vserver si-8040-test-02 -unix-user-name c136758

1234567

### Check Windows to Unix mapping:

diag secd name-mapping show –node <node> -vserver <vserver> -direction win-unix <username>

**Example**

eg-si-clsn-e01::\*> diag secd name-mapping show -node eg-si-clsn-e01-h02 -vserver si-8040-test-02 -direction win-unix -name ten\uc136758

ten\uc136758 maps to c136758

### Check Windows to Unix mapping:

diag secd name-mapping show –node <node> -vserver <vserver> -direction unix-win <username>

**Example**

eg-si-clsn-e01::\*> diag secd name-mapping show -node eg-si-clsn-e01-h02 -vserver si-8040-test-02 -direction unix-win -name c136758

c136758 maps to ten\uc136758