THOMSON REUTERS

NetApp
Go further, faster

7MTT – Multi-Protocol 7-Mode to CDOT Work Instructions

Authors: Ian Daniel

Contributors:

Document Version: V1.1
Date: March 2017
Status: Draft

Contents

1 Introduction

1.1 Management Summary

This document details the process used to migrate a Multi-Protocol vfiler from 7mode to CDOT with 7MTT.

- Servers connected via NFS or SMB

- One Vserver per application
- Up to 128 Vservers per node
- One LIF per Vserver with NFS or SMB

- FAS80xx or FAS32xx cluster with 2 to 8 nodes
- Single node cluster for SnapVault backup systems

- DS2246 or DS4246 SAS attached disk shelves
- Multiple volumes per Vserver
- LIFs and Volumes on same node for direct path I/O

1.2 Change History

Ver	Date	Author	Key Changes
1	May 2016	Ian Daniel	Initial Version
1.1	March 2017	Ian Daniel	Added AV settings

1.3 Distribution List

Name	Role
Storage Support	
Storage Delivery	

1.4 References

No.	Title	Location
1	cDOT Naming Standards	Link
2	cDOT AV	Link
3	cDOT Vserver Creation	Link
4	cDOT Consolidated Build Standards	Link
5	cDOT Replication Deployment Guidelines	Link
6		
7		

1.5 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.
7MTT	7mode Transition Tool – A tool used to migrate from 7mode to CDOT
WFA	OnCommand Workflow Automater – An automation framework application from NetApp, used for storage provisioning.

2 Additional 7-Mode Multi-Protocol Configuration To Migrate To cDOT

2.1 Domain Users and Groups

There are often Domain users and Groups configured on a 7-Mode CIFS vfiler, these can be displayed as shown on a group-by-group basis and are transferred as part of the 7MTT migration process. To check members of a group you can use the following command. It is recommended to check all the groups.

Example

```
eag-laborf-nas6210ht-1> vfiler run si-nastest-01   useradmin domainuser list -g administrators

===== si-nastest-01

List of SIDS in administrators
S-1-5-21-1789992843-188582088-1440544181-131073
S-1-5-21-1789992843-188582088-1440544181-500
S-1-5-21-1042883198-748202677-1346798384-512
S-1-5-21-2012327785-2259879848-3711903672-512
S-1-5-21-2012327785-2259879848-3711903672-56518
S-1-5-21-2012327785-2259879848-3711903672-55774
For more information about a user, use the 'cifs lookup' and 'useradmin user list' commands.
```

You can determine the actual names of the displayed SIDs as follows. This can be useful when checking what was migrated across to cDOT as it will not display SIDs.

Example

```
eag-laborf-nas6210ht-1> vfiler run si-nastest-01  cifs lookup S-1-5-21-2012327785-2259879848-3711903672-
55774

===== si-nastest-01
name = TEN\M-Storage-admins.G

eag-laborf-nas6210ht-1> vfiler run si-nastest-01  cifs lookup S-1-5-21-2012327785-2259879848-3711903672-
56518

===== si-nastest-01
name = TEN\M-EaganServerAdmins

eag-laborf-nas6210ht-1> vfiler run si-nastest-01  cifs lookup S-1-5-21-2012327785-2259879848-3711903672-512

==== si-nastest-01
name = TEN\Domain Admins

eag-laborf-nas6210ht-1> vfiler run si-nastest-01  cifs lookup S-1-5-21-1042883198-748202677-1346798384-512

===== si-nastest-01
name = TLR\Domain Admins

eag-laborf-nas6210ht-1> vfiler run si-nastest-01  cifs lookup S-1-5-21-1789992843-188582088-1440544181-500

===== si-nastest-01
name = SI-NASTEST-01\administrator

eag-laborf-nas6210ht-1> vfiler run si-nastest-01  cifs lookup S-1-5-21-1789992843-188582088-1440544181-
131073

===== si-nastest-01
name = SI-NASTEST-01\root
```

2.2 Share Permissions

There are often Domain users and Groups configured on a 7-Mode CIFS share, these can be displayed as shown and will be transferred by 7MTT at migration time.

```
eag-laborf-nas6210ht-1> vfiler run si-nastest-01  cifs shares

===== si-nastest-01
Name          Mount Point                      Description
----          -----------                      -----------
ETC$          /vol/si_nastest_01_root/etc      Remote Administration

                        BUILTIN\Administrators / Full Control
HOME          /vol/si_nastest_01_root/home     Default Share
                        everyone / Full Control
C$            /                                Remote Administration
                        BUILTIN\Administrators / Full Control
TESTSHARE01   /vol/cifsmig01/share01
                        everyone / Full Control
                        TEN\M-Storage-admins.G / Full Control
                        TEN\uc136758 / Change
                        TLR\Domain Admins / Full Control
```

3 7-Mode to CDOT Multi-Protocol Migration

3.1 High Level Migration Steps

Task	Owner
Create SVM and volume	Storage
Initialize snapmirror replication	Storage
Stop application during maintenance window	Application
Unmount source volumes during maintenance window	Platform
Final snapmirror sync/break during maintenance window	Storage
Update server mount info, e.g. change is server \\server\path	Platform
Mount new share(s) during maintenance window	Platform
Start application	Application
Verify	Application/Platform

3.2 Pre-requisites

- **Ensure version of 7MTT is 2.3 or higher**
- **Ensure vfiler being migrated is not currently exceeding the 6K IOPS threshold unless it is moving to a dedicated controller.**
- **Ensure snapshot autodelete is disabled during the migration process for both source and destination.**
- Add the CDOT vserver name (not IP) to the source systems /etc/snapmirror.allow file
- Add the cDOT cluster ICL IP Addresses to the snapmirror.access option or the snapmirror.allow file on the source 7-Mode system prior to migration.
- Confirm the target aggregate has sufficient capacity
- Confirm the source volume is 64 bit
- Register the target vserver hostname in DNS
- Ensure the target vserver is in the required AD domain
- Ensure the target vserver has NFS enabled
- Ensure the target vserver lif is enabled for CIFS and NFS (if not delete and re-create)
- Ensure the target vserver allows both CIFS and NFS
- Ensure the destination cluster has AV enabled and the destination vserver has scanning turned on
- Make note of service accounts on the source so they can be created in destination

- Confirm there is network connectivity between the source and target
- Make note of qtree quotas sizes so they can be applied in destination
- Make note of the source volume language
- Make note of the backup volume size

3.3 Vserver and LIF creation

3.3.1 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
```

3.3.2 Create LIF with default route and failover group

```
network interface create -vserver <vsname> -lif <vsname>-lif<lif#> -role data -
data-protocol <protocols> -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>
```

3.4 DNS configuration

3.4.1 Setup DNS on a Vserver

```
vserver services dns create -vserver <vsname> -domains <domainname> -name-
servers <comma_separate_name_server_list>
```

vserver services dns show

3.4.2 Setup DNS on Cluster Admin Vserver

For ONTAP 8.2.x you need to make sure that whatever DNS domains are on your data vservers also get added to the admin vserver as DNS lookups can also be done via that vserver.

```
vserver services dns modify -vserver <admin_vsname> -domains <domainnames>
```

```
vserver services dns show
```

3.5 Create service account if required

```
security login role create -role <ROLE_NAME> -cmddirname "<COMMAND>" -access
<ACCESS_TYPE> -vserver <vserver>   #Repeat this command for each required cDOT command
```

```
security login create -username <USER_NAME> -application ontapi -authmethod
<AUTHENTICATION_METHOD> -role <ROLE_NAME> -vserver <vserver>
```

3.6 Enable CIFS Protocol

3.6.1 Enable CIFS

```
cifs create -cifs-server <vsname> -domain <ad_domain> -ou CN=Computers -status-admin up -vserver <vserver>

cifs show
```

3.7 Enable Anti-Virus Scanner Pool

3.7.1 Set Primary Pool

```
vscan scanner-pool apply-policy -scanner-pool SCANNER_POOL -vserver VSERVER_NAME -scanner-policy primary
```

3.7.2 Enable vscan

```
vscan enable -vserver VSERVER_NAME
```

3.8 Enable NFS Protocol

3.8.1 Enable NFS

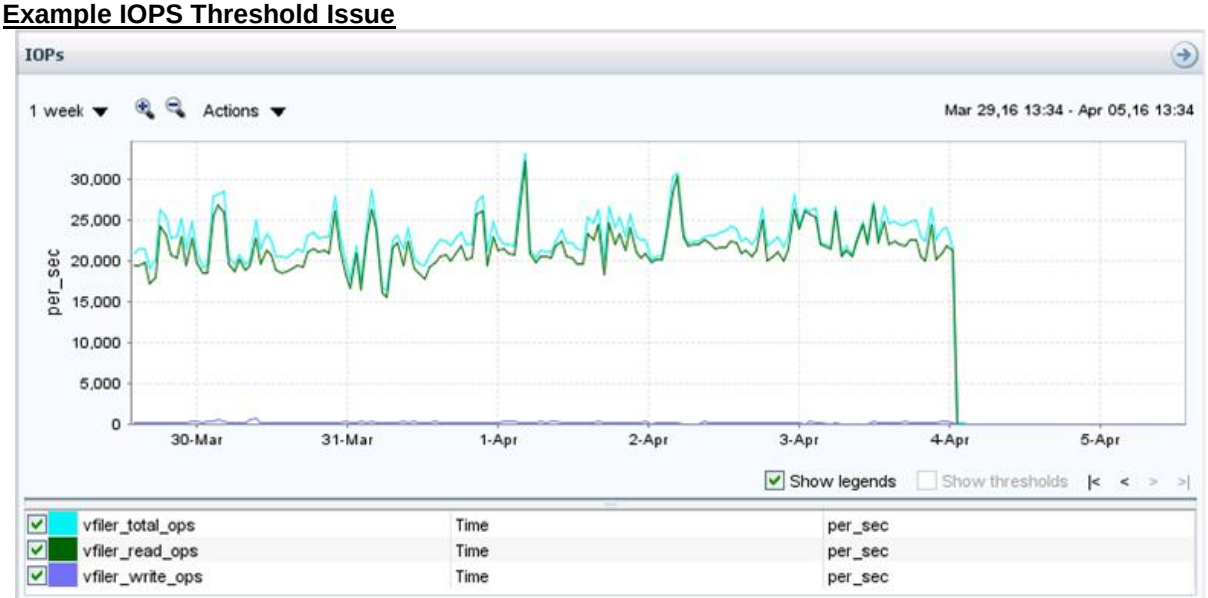
```
vserver nfs create -vserver <vsname> -access true -v3 enabled

vserver nfs show
```

3.9 Check Current IOPS In Use Prior To Migration – Shared Migrations ONLY

If the volume is seeing large periods of time over 6000 IOPs/sec please raise the flag that it needs to be looked at as 6000IOPs/sec will be the most they can use on cDOT due to QOS.So there is a high probability that the customer will feel the effect from this.

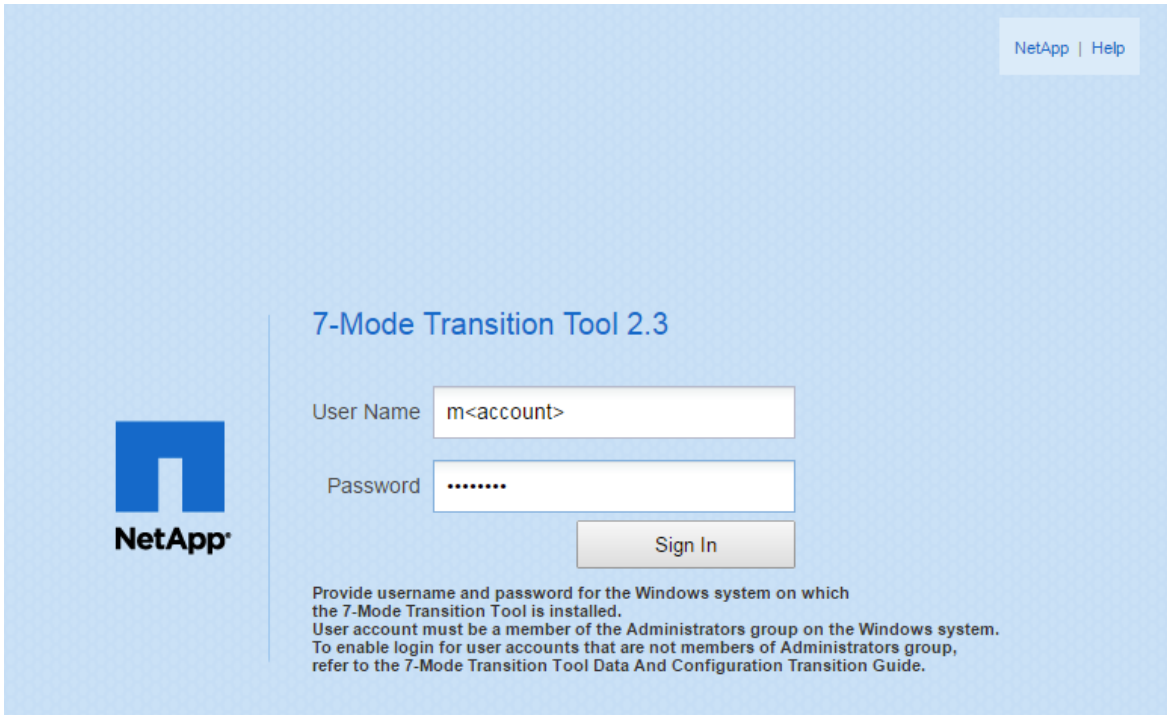
Example IOPS Threshold Issue



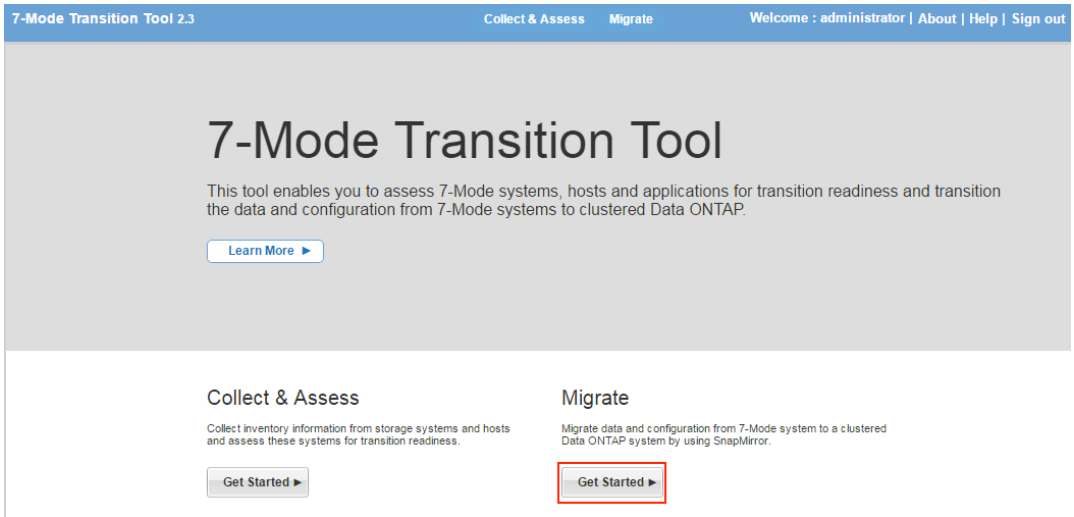
3.10 Start the Migration

3.10.1 Login to 7MTT

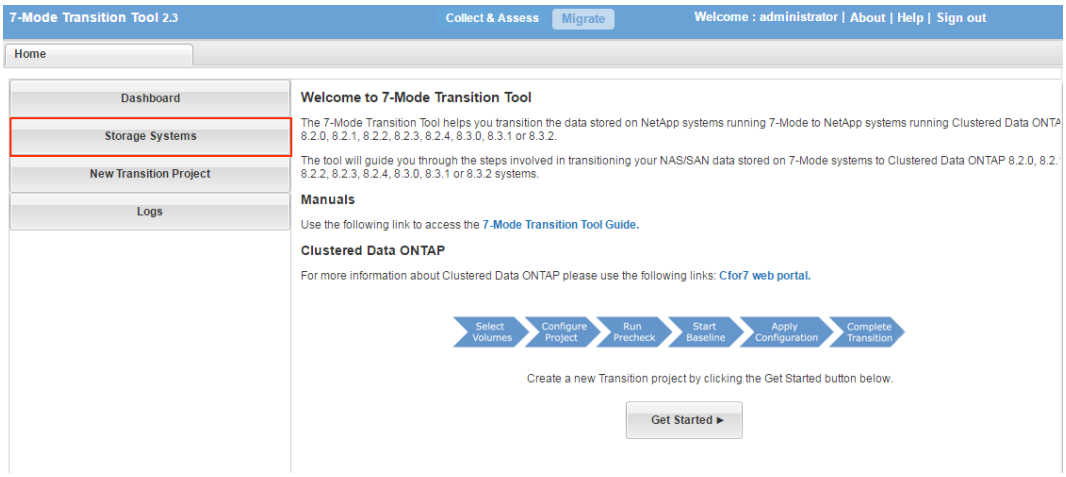
Connect the 7MTT (https://<7MTT_Server>:8443/transition) tool via web browser



Once logged in CLICK Get Started under Migrate'



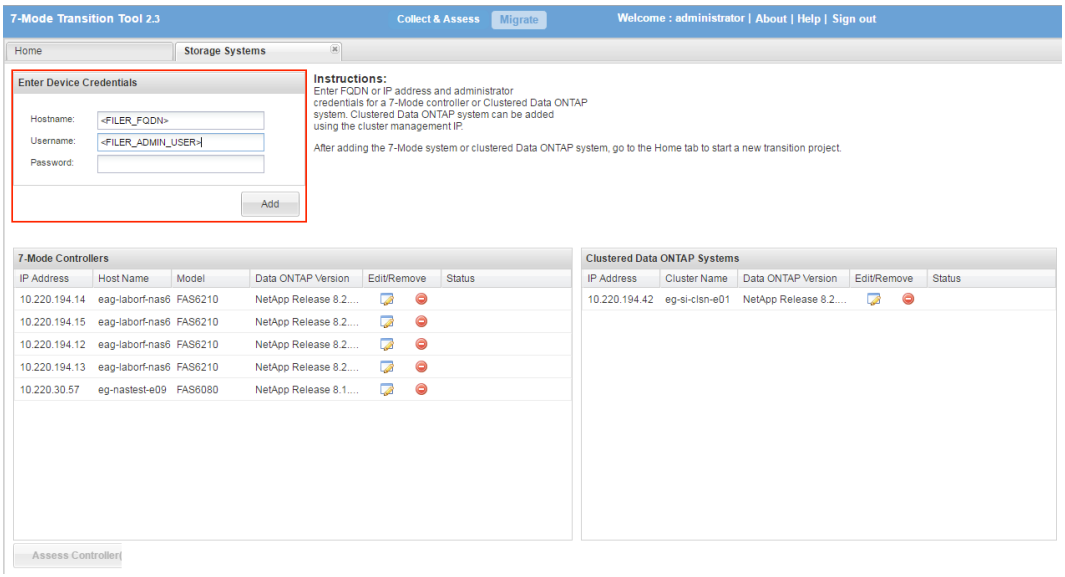
CLICK on the 'Storage System' button in the left pane:



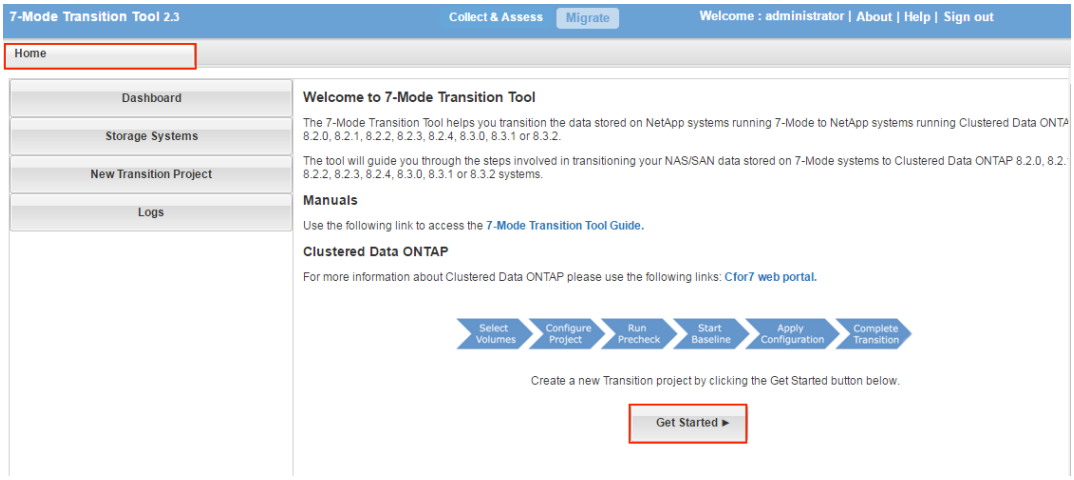
ADD storage systems to 7MTT (execute this step for the source and target storage systems):

ENTER the FQDN of the filer

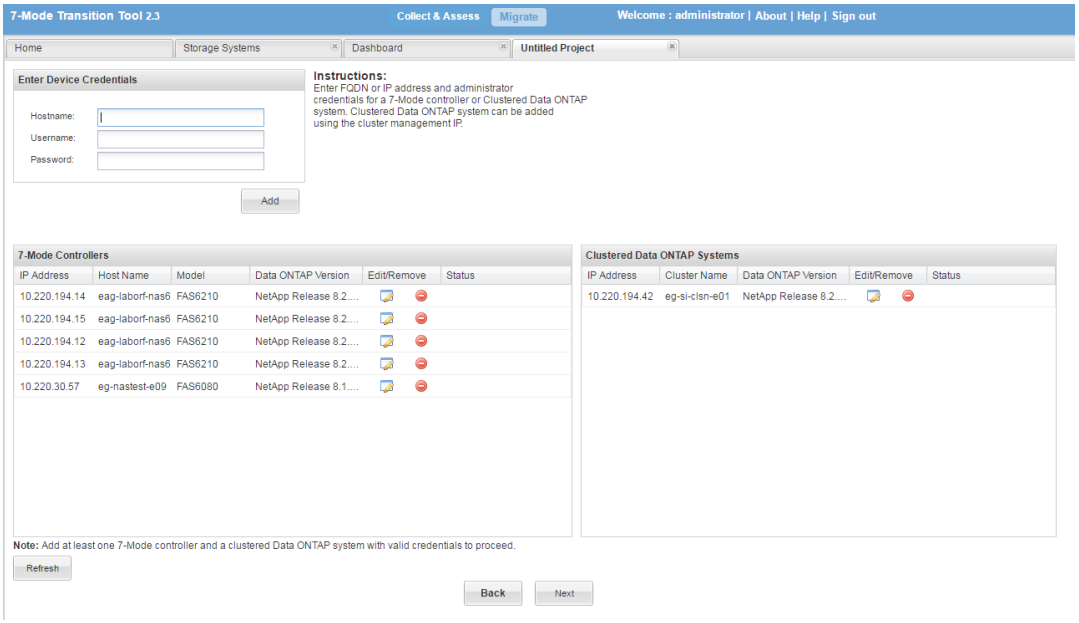
CLICK ADD



CLICK the ‘HOME’ tab -> CLICK ‘Get Started’



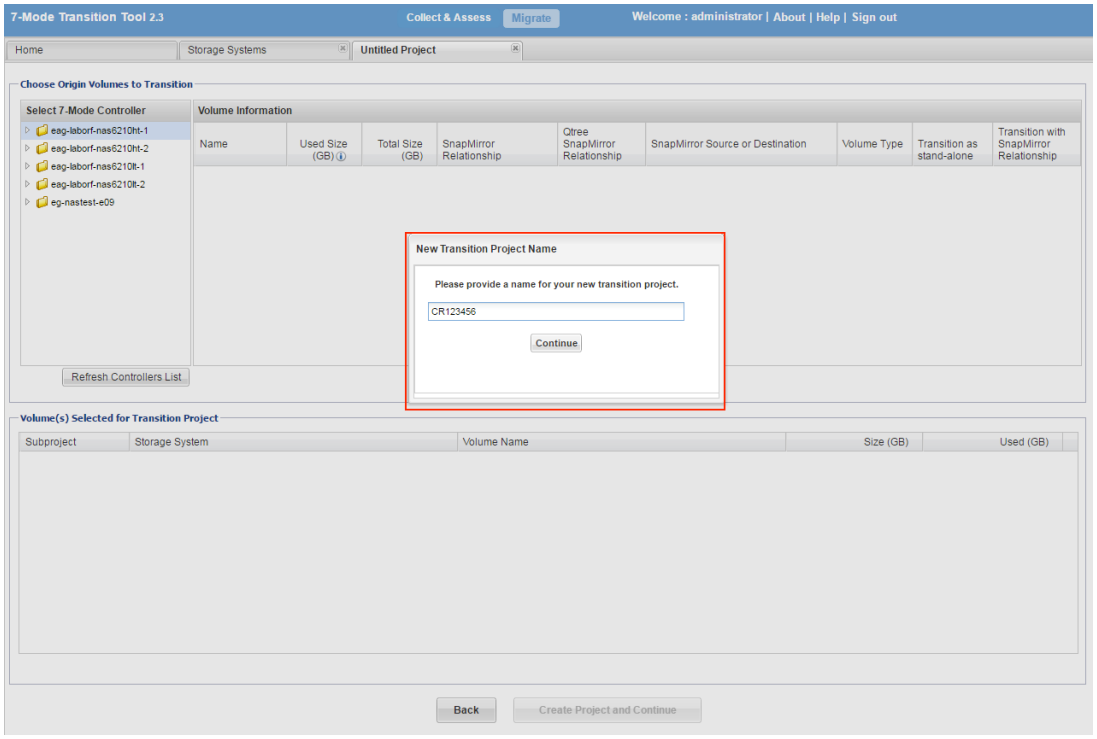
CONFIRM that the source and destination storage systems are listed



CLICK ‘Next’

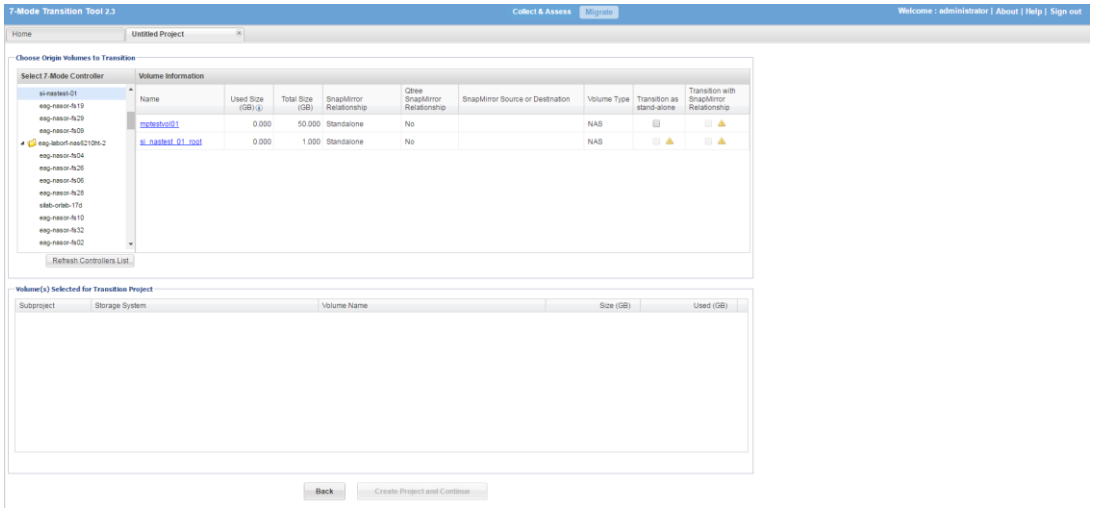
ENTER a name for the project

CLICK ‘Continue’



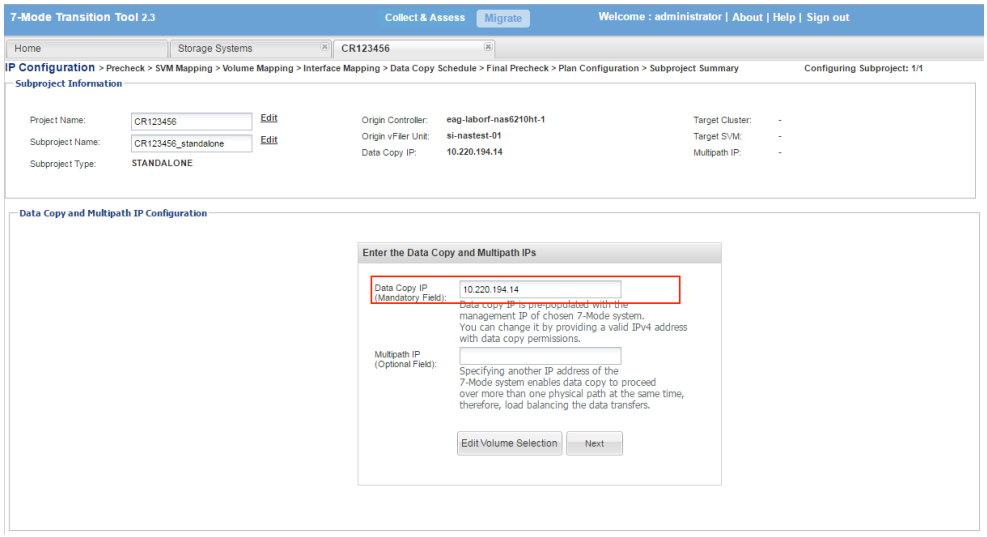
SELECT the source vfiler and volume(s):

CLICK ‘Create Project and Continue’



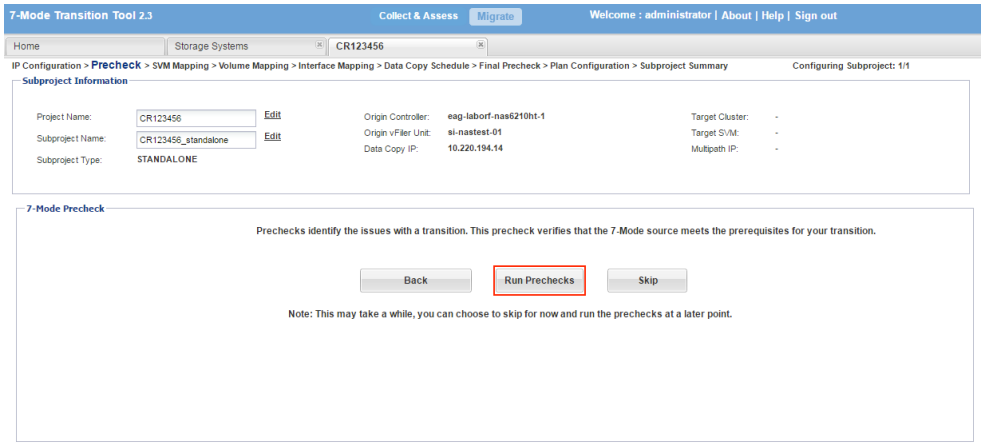
ENTER an IP to be used for replication traffic on the source filer

CLICK ‘Next’



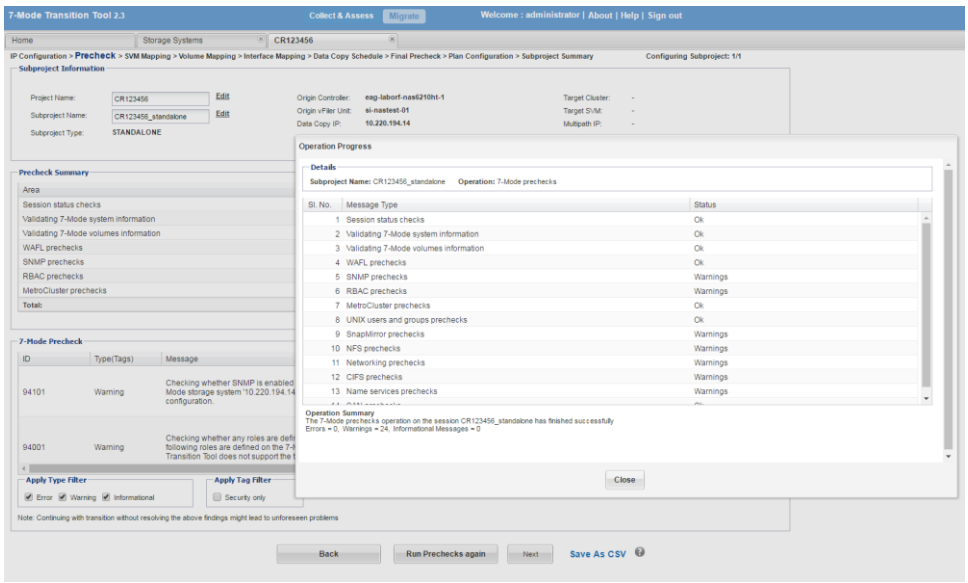
The next window will ask if you want to run pre-check.

CLICK ‘Run Prechecks’



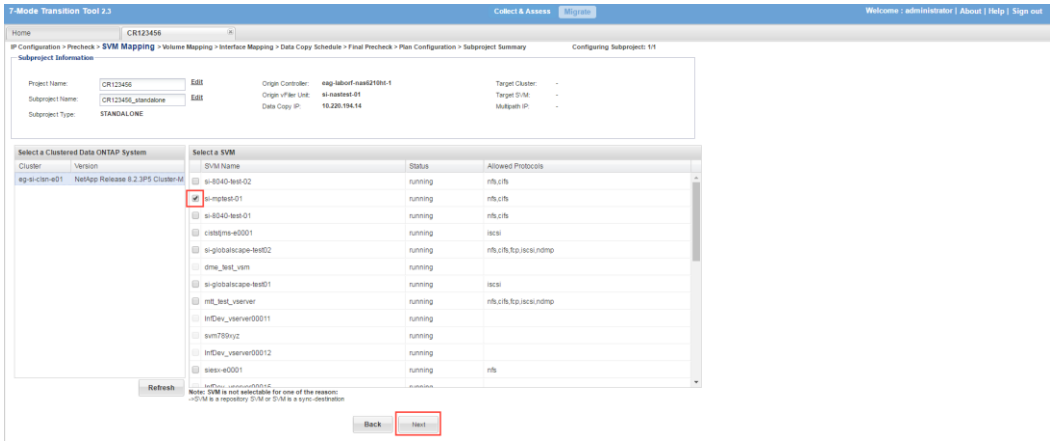
Review the Report. You can ignore the warnings listed below. Resolve errors if they appear.

CLICK ‘Close’ and then click Next’



SELECT a target vserver

CLICK ‘Next’



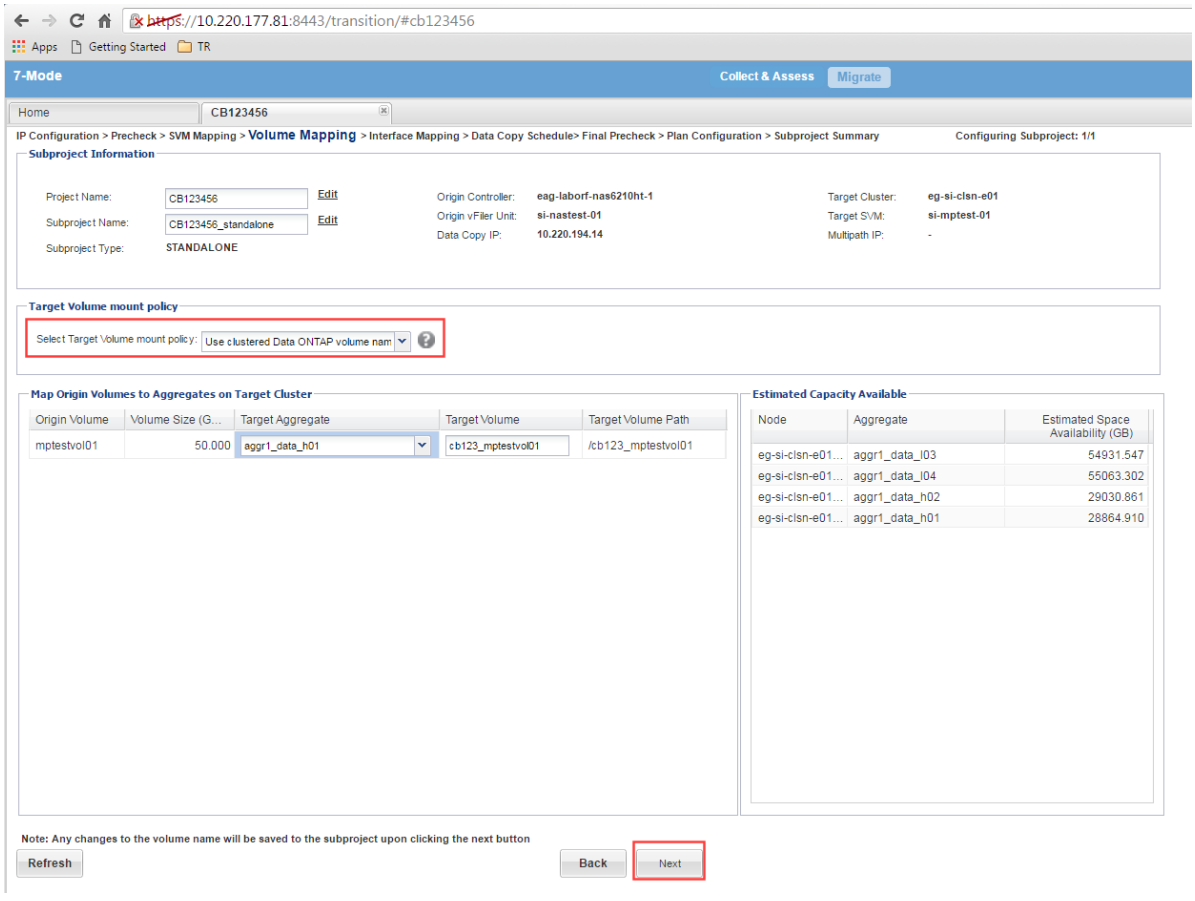
IMPORTANT: Make sure you enter the correct information in the next section! This version of 7MTT allows you to set junction path = volume name, this is the DCO standard. But, you need to modify the junction-path after the cut-over manually in older versions of 7MTT.

ENTER the destination aggregate

ENTER the destination volume name

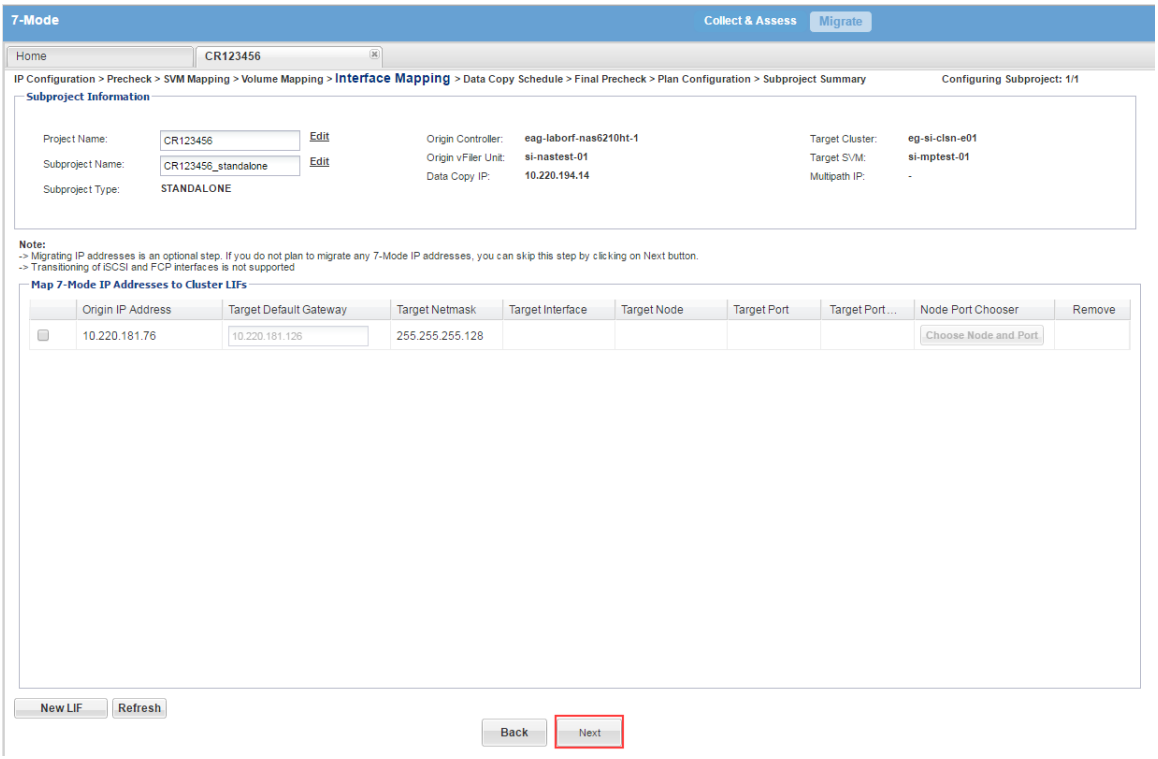
SELECT ‘Use Clustered OTAP volume name’ from ‘Target Volume Mount Policy’

CLICK ‘Next’



NOTE: We are not migrating IP addresses

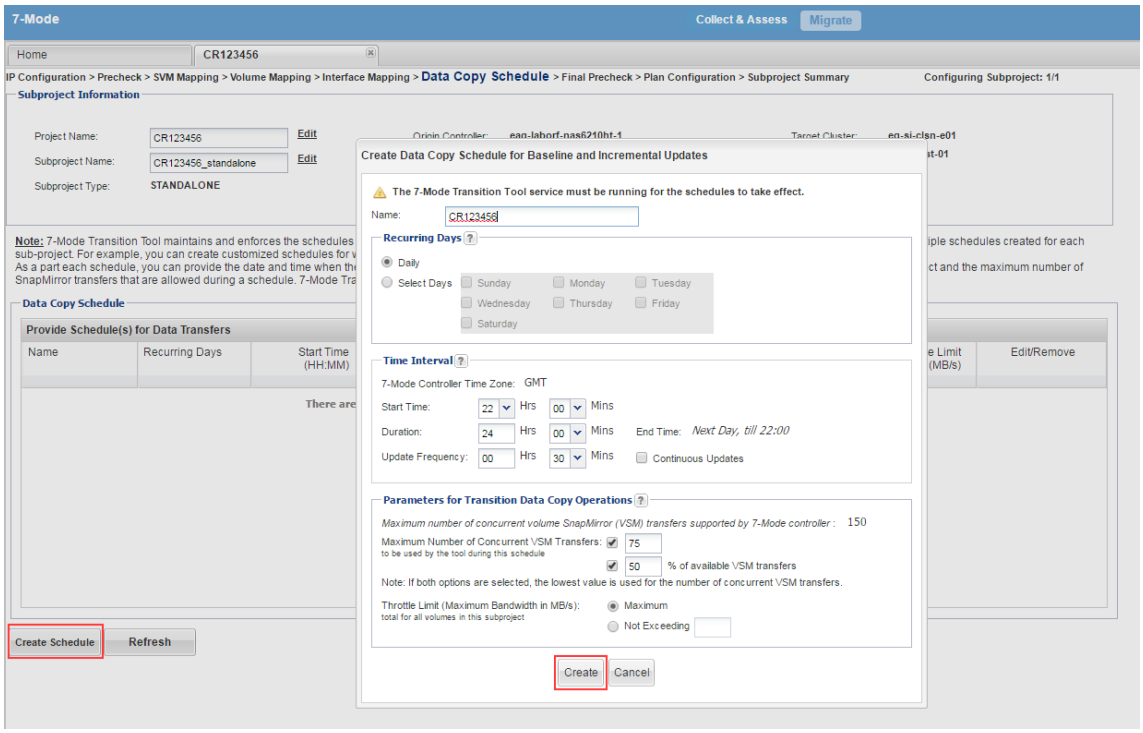
CLICK ‘Next’



CLICK ‘Create Schedule’, a popup box will appear

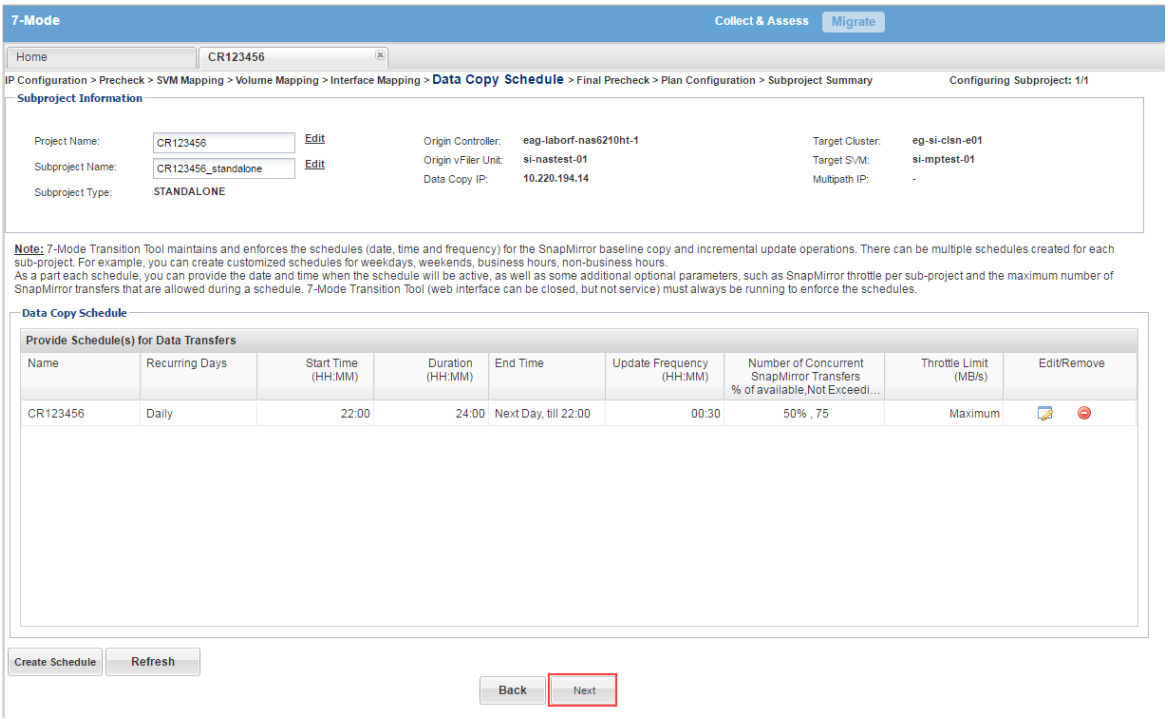
ENTER a replication schedule (run off hours)

CLICK CREATE



The newly created schedule will appear

CLICK ‘Next’

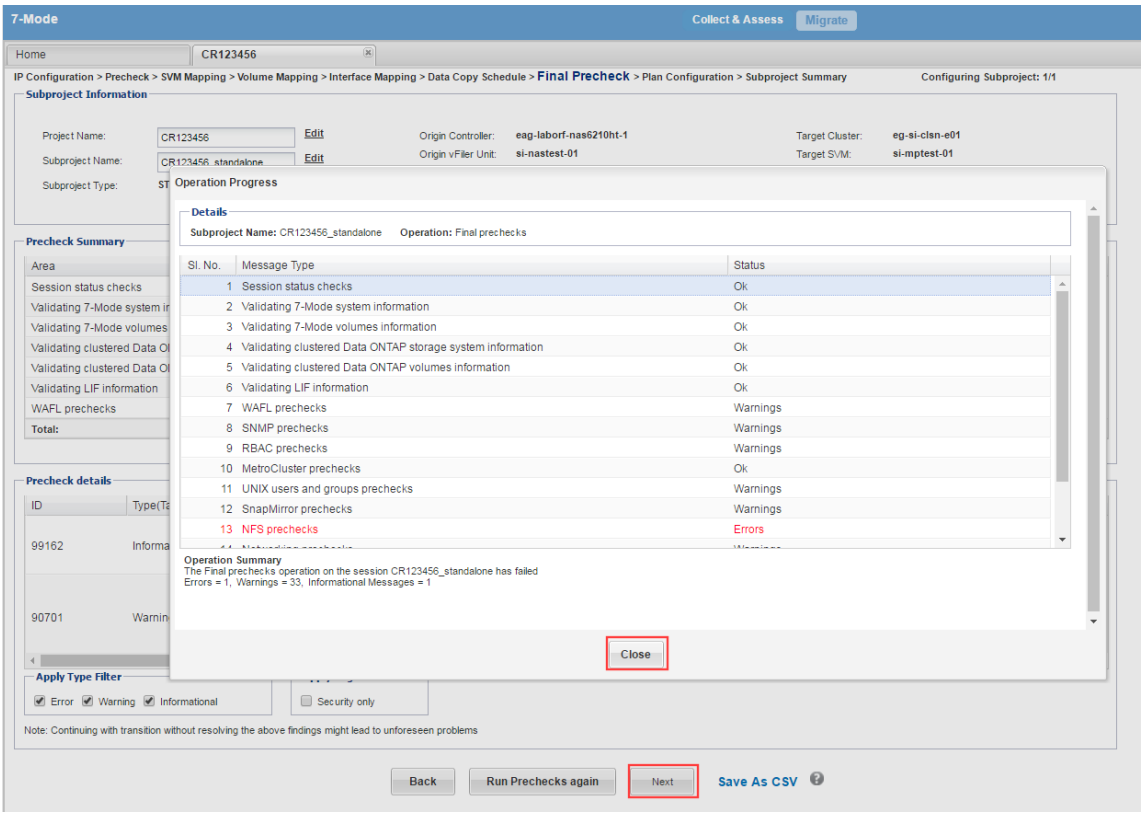


RUN PreCheck and make sure there are no errors

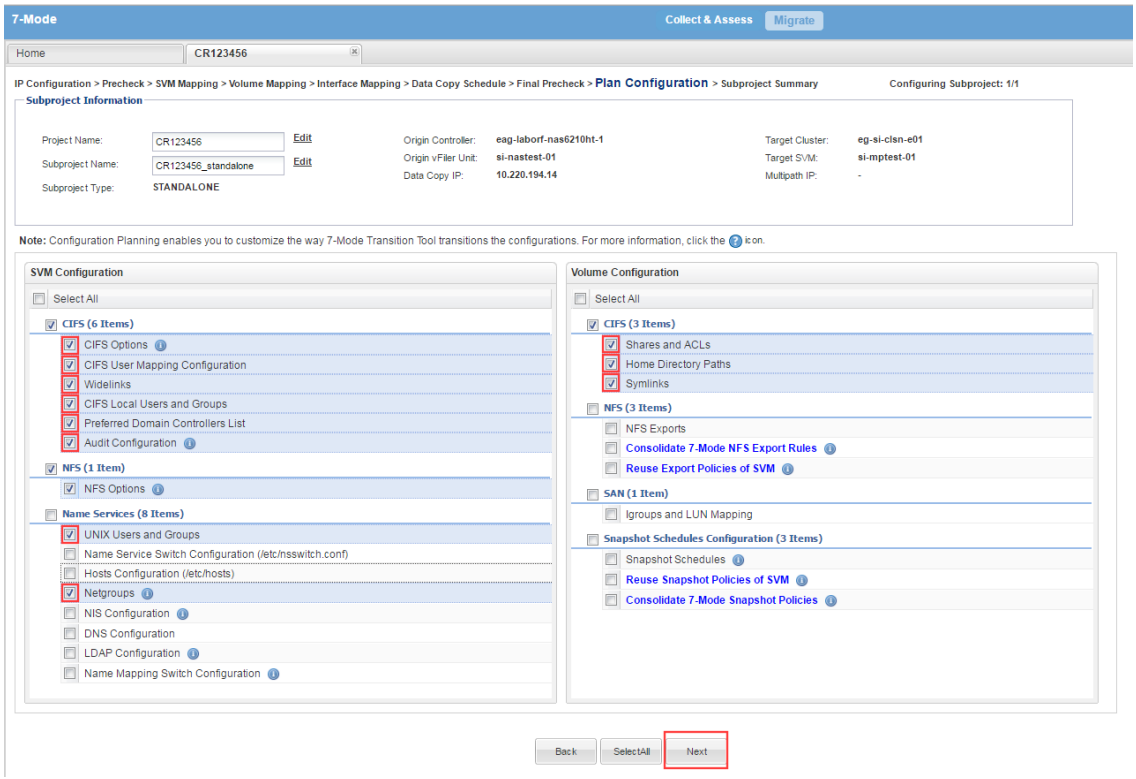
CLICK ‘Run Precheck’; REVIEW the output

CLICK ‘Close’

CLICK ‘Next’



Modify the options to ensure all correct data is transferred to the destination vserver.



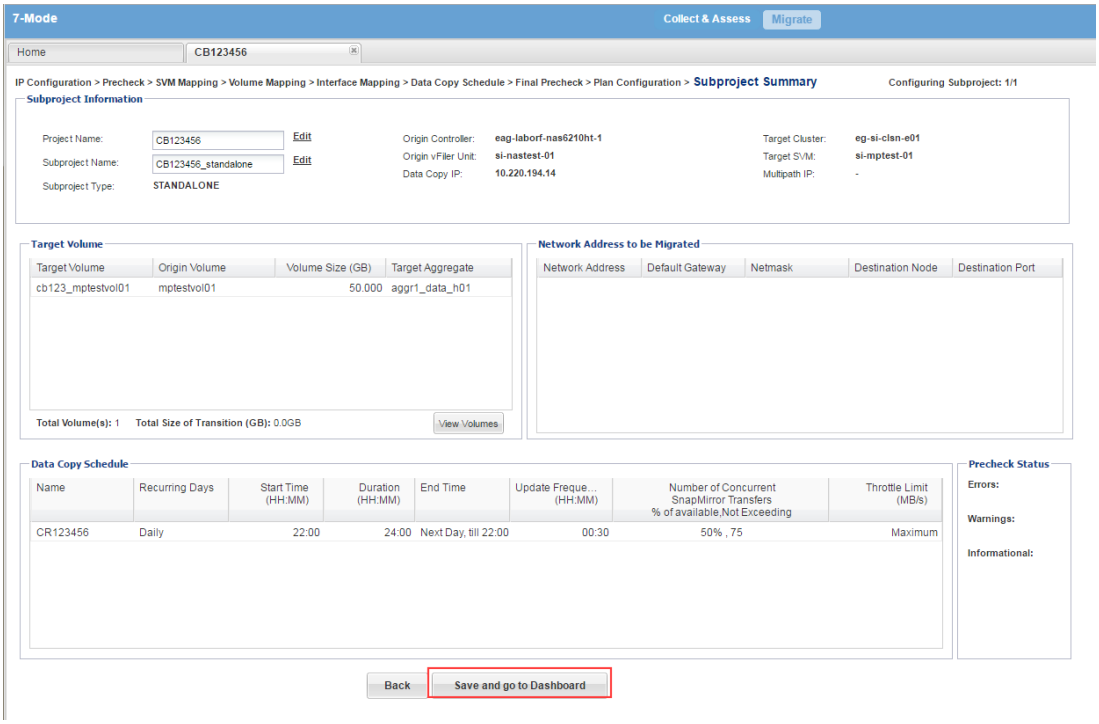
Relevant Options Description

Option	Description	Set
CIFS Options	If the CIFS options are not selected for transition, the following 7-Mode CIFS options are not transitioned to the clustered Data ONTAP: cifs.gpo.enable, cifs.smb2.enable, cifs.smb2.signing.required, cifs.wins_servers, cifs.grant_implicit_exe_perms, cifs.restrict_anonymous.	Yes
CIFS User Mapping Configuration	Copies over usermap.cfg entries	Yes
Widelinks	Copies any widelinks that may be in use	Yes
CIFS Local Users and Groups	Copies local users and groups across	Yes
Preferred Domain Controller List	Copies the preferred DC list across	Yes
Audit Configuration	If the CIFS audit configuration is not selected for transition, the audit configuration is not transitioned even if the audit path was specified.	Yes
Shares and ACLs	Copies all share and ACL information across	Yes
Home Directory Paths	Copies home directory paths across	Yes
Symlinks	Copies any symlink configuration across	Yes
NFS Options	If the NFS options are not selected for transition, the following 7-Mode NFS options are not transitioned to the clustered Data ONTAP: nfs.udp.xfersize, nfs.v4.id.domain, nfs.v4.acl.max.aces, nfs.tcp.xfersize, nfs.rpcsec.ctx.high, nfs.rpcsec.ctx.idle, nfs.response.trigger, wafl.default_nt_user, nfs.mount_rootonly, nfs.tcp.enable, nfs.udp.enable, nfs.response.trace, nfs.v4.read_delegation, nfs.v4.write_delegation, nfs.v4.acl.enable, nfs.vstorage.enable, nfs.v3.enable, nfs.v4.enable.	Yes
UNIX Users and Groups	Copies local user/group information	Yes
Name Service Switch Configuration (/etc/nsswitch.conf)	Copies nsswitch.conf across	No
Host Configuration (/etc/hosts)	Copies host entries over	No
Netgroups	If Netgroups are selected for transition, all the existing	Yes

	Netgroups on the target SVM are replaced with the Netgroups transitioned from the 7-Mode. If there are no Netgroups configured in the '/etc/netgroups' file of the 7-Mode system, then existing Netgroups on the target SVM are retained	
NIS Configuration	If NIS configuration is not selected for transition, NIS is not added to the name service switch on the target SVM.	No
DNS Configuration	Copies DNS configuration over	No
LDAP Configuration	If LDAP configuration is not selected for transition, LDAP is not added to the name service switch and Name mapping switch on the target SVM.	No
Name Mapping Switch Configuration	If LDAP configuration is not selected for transition, LDAP is not added to the name mapping switch on the target SVM even if 7-Mode has the option 'ldap.usermap.enable' set to on. You must manually add LDAP to the name mapping switch after LDAP is configured on the target SVM.	No
NFS Exports	Create export policies on destination	No
Consolidate Export Rules	If this option is selected, only one NFS export policy is created on the target SVM for all the volumes and qtrees with matching 7-Mode export rules. And the created NFS export policy is used to export all those volumes/qtrees on the target SVM. If the 'Reuse the export policies of SVM' option is selected, and if there is a matching NFS export policy existing on the target SVM, the pre-existing policy is reused rather than creating a new export policy.	No
Re-Use Export Policies	If this option is selected, and if there is a pre-exisitng NFS export policy that matches with 7-Mode export policy, the pre-exisitng export policy is reused rather than creating a new export policy.	No
Snapshot Schedules	If the Snapshot schedules are not selected for transition, Snapshot schedules of 7-Mode volumes are not transitioned to clustered Data ONTAP and the 'default' Snapshot policy of the target SVM is assigned to the transitioned volumes.	No
Reuse Snapshot Policies of SVM	If this option is selected, and if there is a pre-exisitng Snapshot policy that matches with 7-Mode Snapshot policy, the pre-exisitng policy is reused rather than creating a new policy.	No
Consolidate 7-Mode Snapshot Policies	If this option is selected, only one Snapshot policy (with all the required schedules) is created on the target SVM for all the 7-Mode volumes with matching 7-Mode Snapshot schedules. And the created Snapshot policy is used for all those volumes on the target SVM. If the 'Reuse Snapshot Policies of SVM' option is selected, and if there is a matching Snapshot policy existing on the target SVM, the pre-existing policy is reused rather than creating a new policy.	No

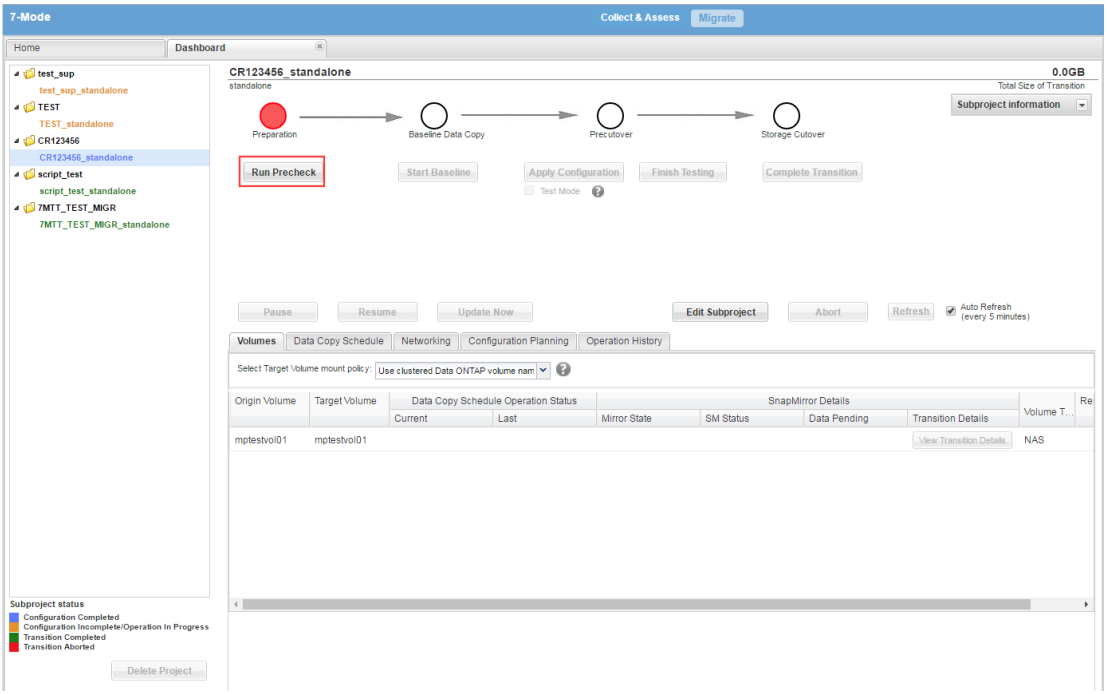
Click Next

CLICK ‘Save and go to Dashboard’

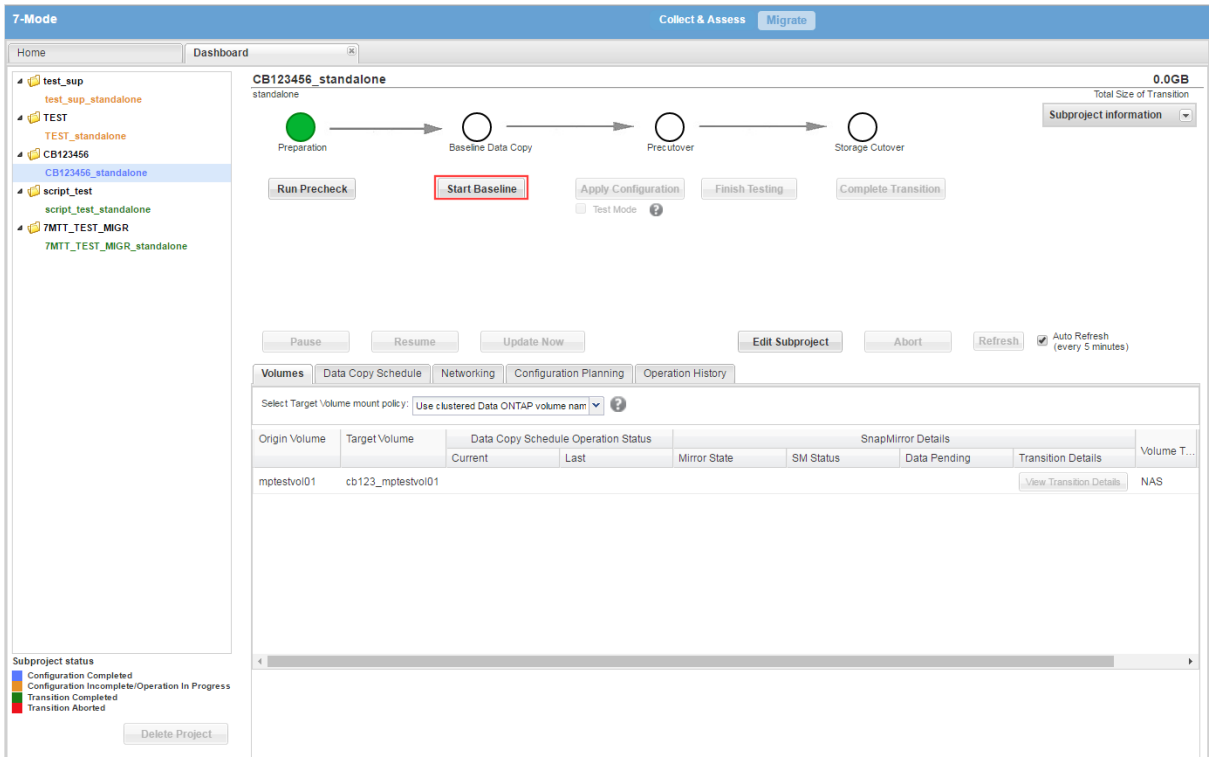


A data transfer workflow will be displayed in the top of the page. The circle above ‘Baseline Data Copy’ will have a white fill color before your first transfer. It will have an orange fill color while the first transfer is running. Then a green fill color after your first successful transfer.

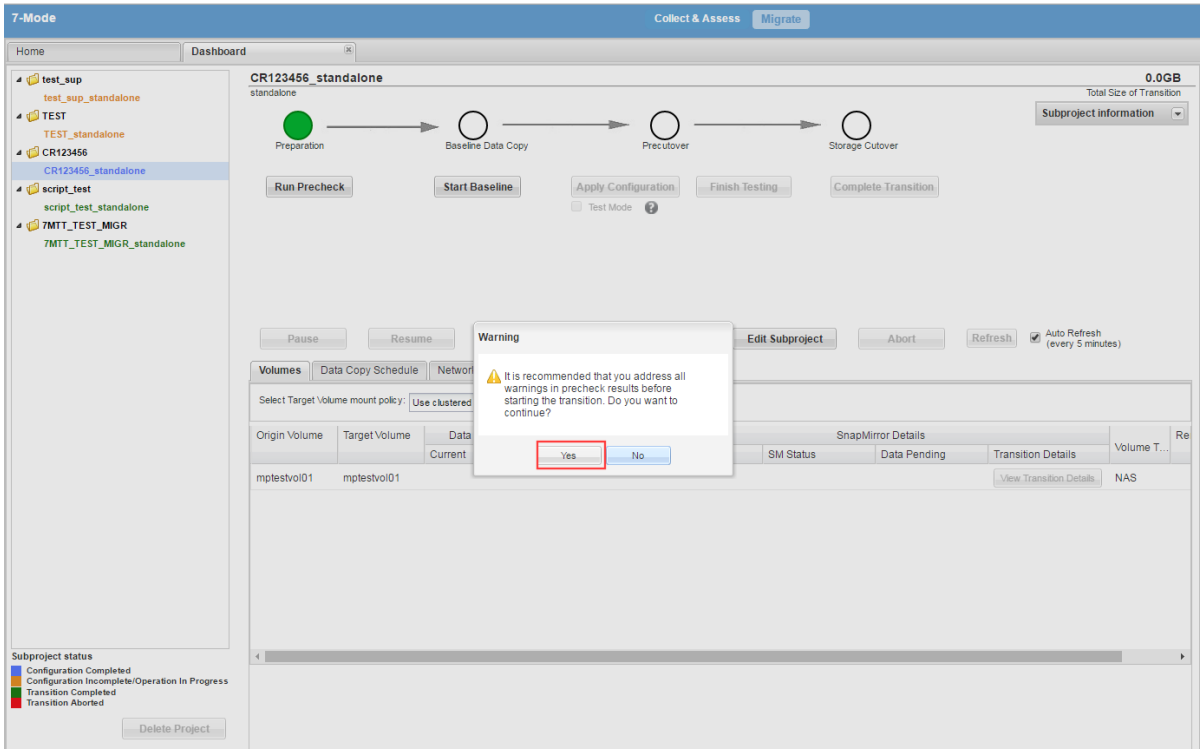
CLICK ‘Run Pre-Check’; REVIEW output



CLICK ‘Start Baseline’

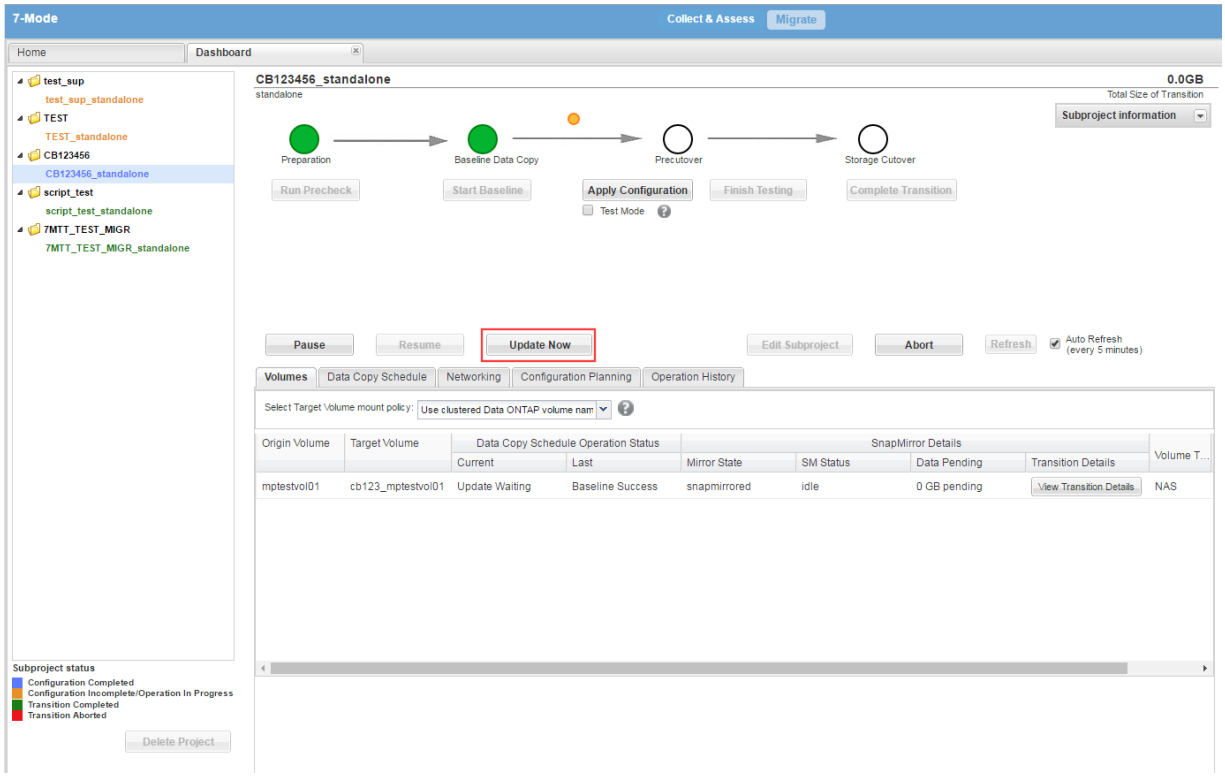


A popup window will appear, CLICK ‘yes’



Execute an update transfer before the cutover window so that you have minimal changes to transfer during the cutover window:

CLICK ‘Update Now’



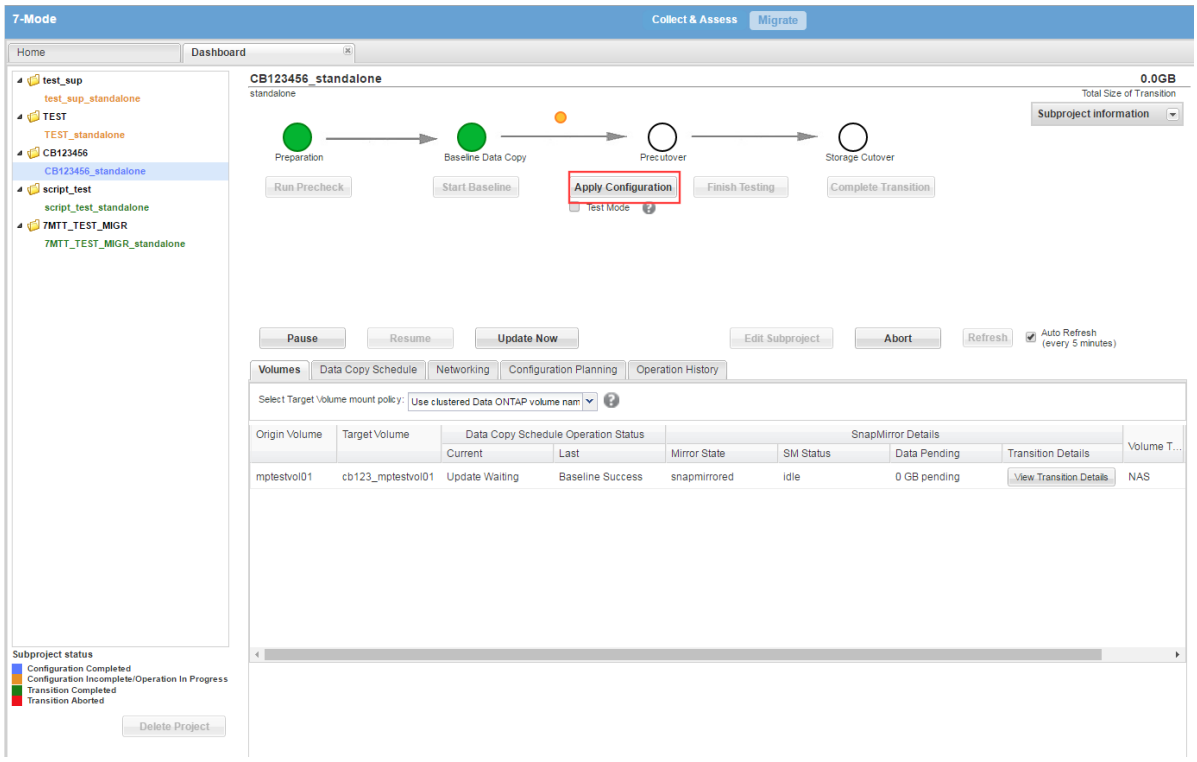
Ensure the steps below are completed during the downtime window:

The application/database has been shut down on all hosts

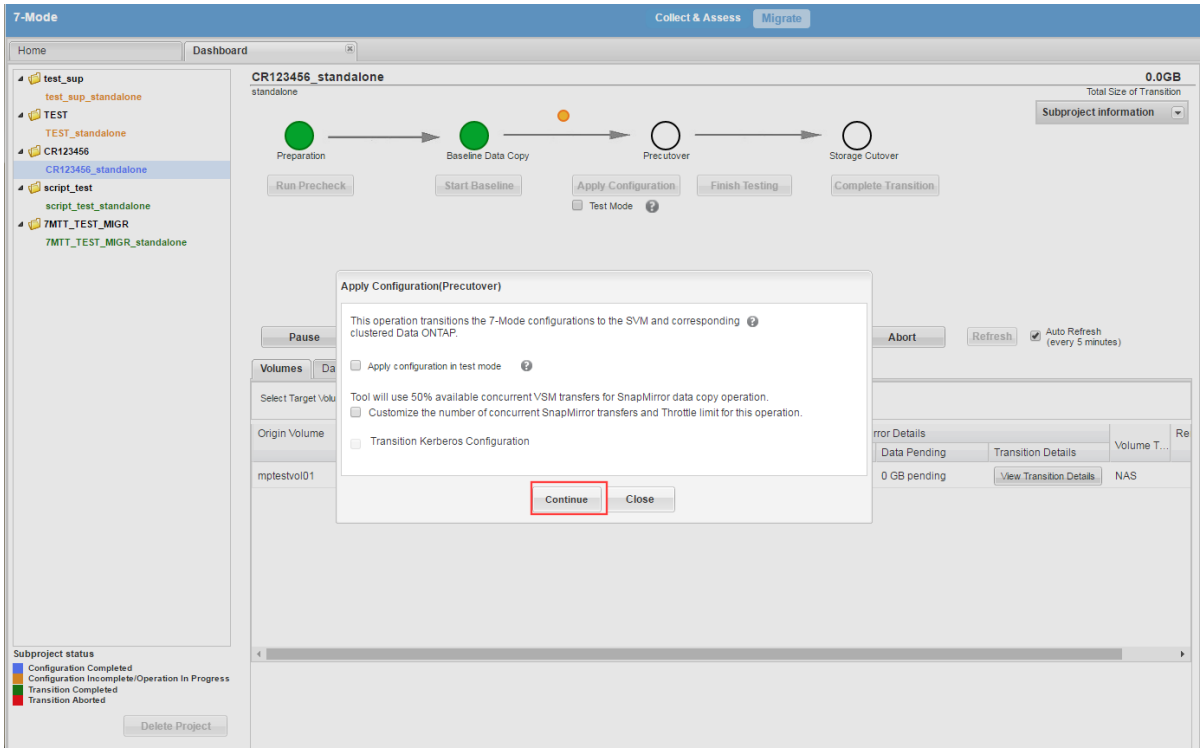
Source shares have been unmounted on all hosts

Start the cutover process:

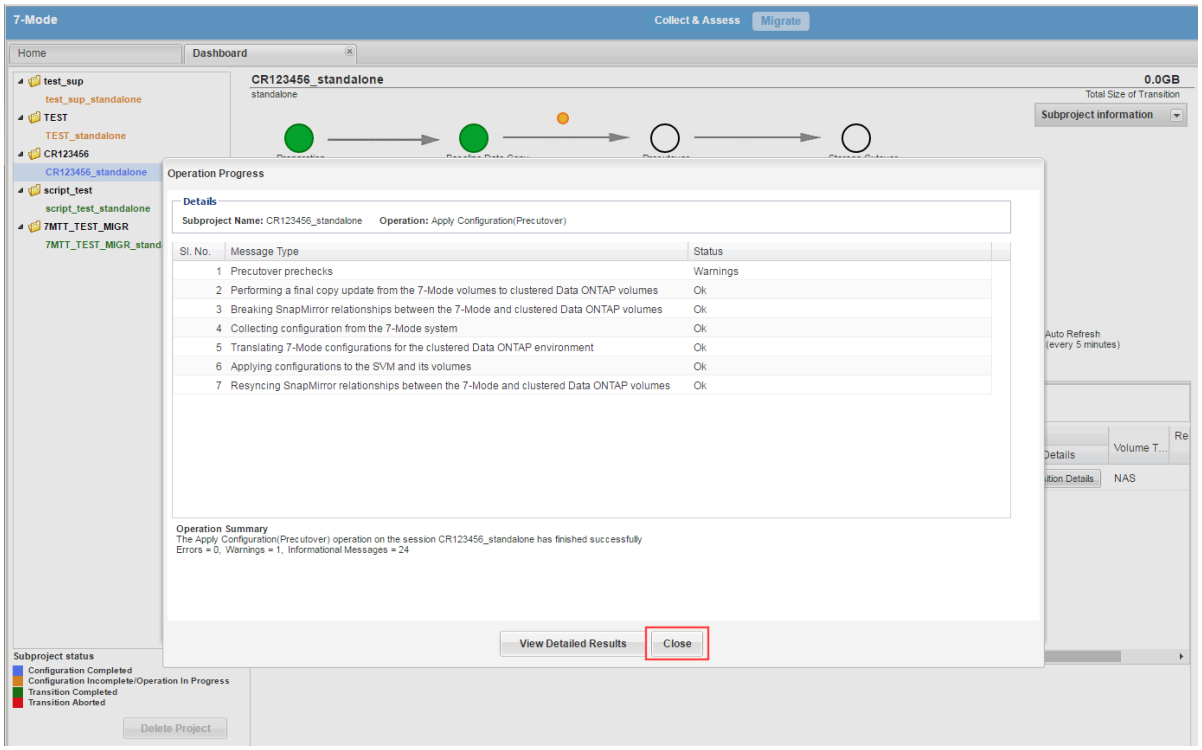
CLICK ‘Apply Configuration’



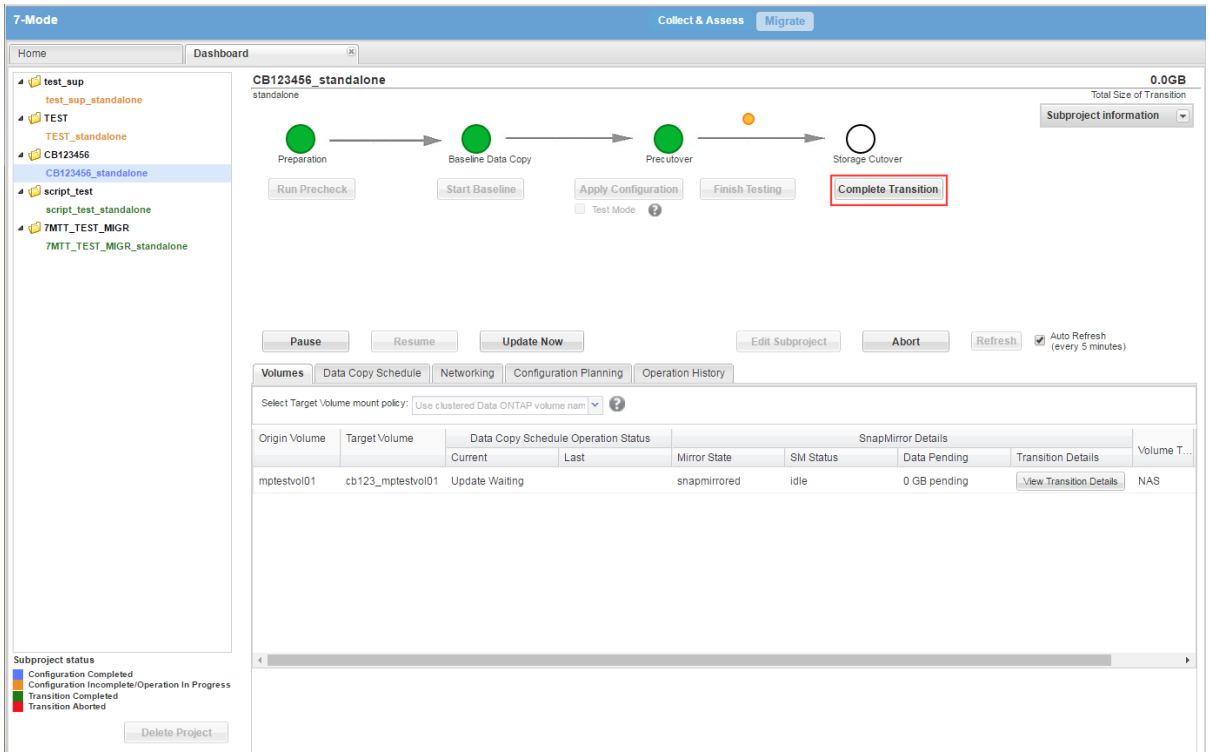
A popup box will appear, CLICK ‘Continue’



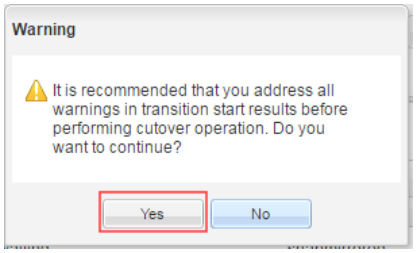
REVIEW log for errors and CLICK ‘Close’



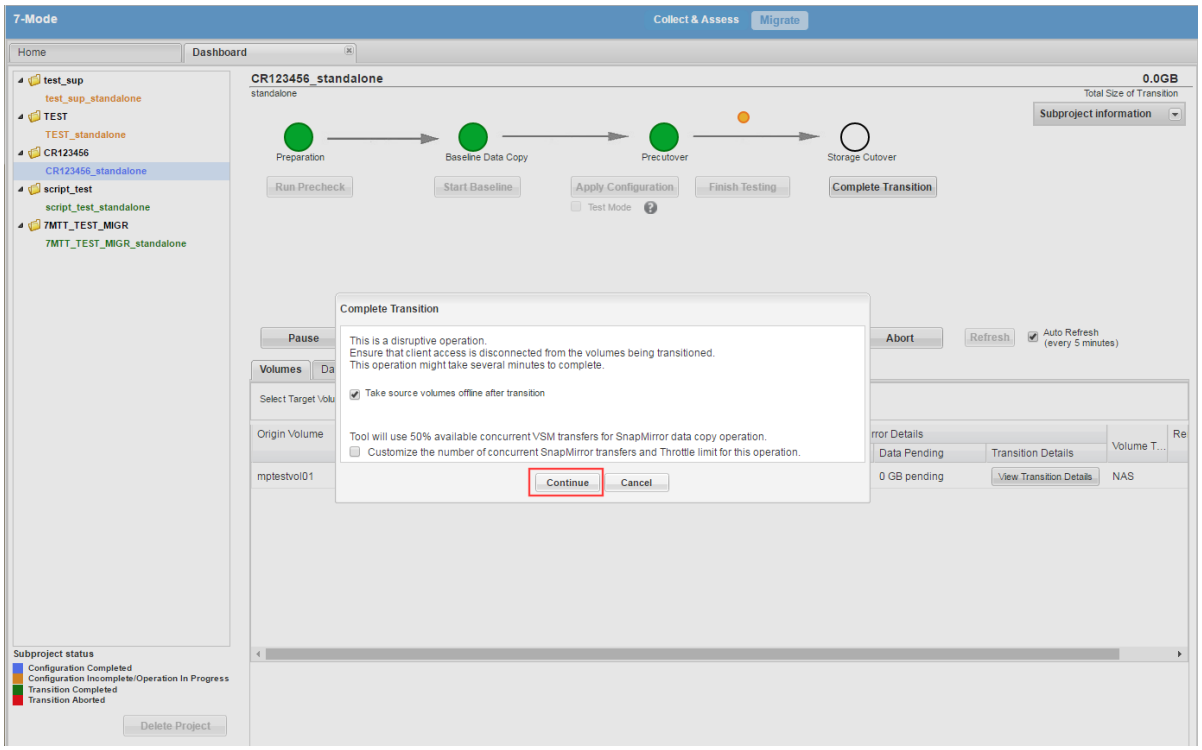
CLICK ‘Complete Transition’



A popup box will appear, CLICK ‘yes’

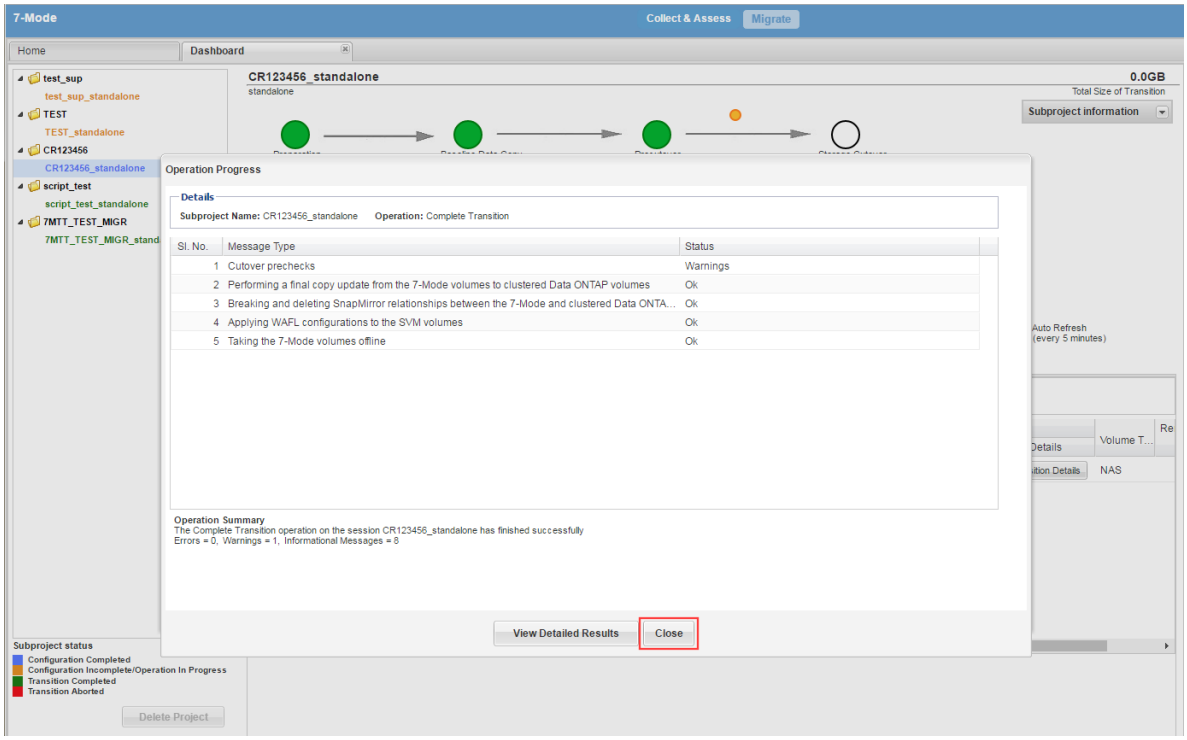


A popup box will appear stating that the source volume will be made offline, CLICK ‘Continue’



REVIEW the log output for a successful transition

CLICK ‘Close’



3.11 Post cut-over activities

3.11.1 Create job schedule and snapshot policy for SNAP volume(s)

```
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>
```

3.11.2 Post Checks

- Check CIFS options were correctly copied across
- Check local users and groups were copied across
- Check shares were correctly created with same permissions
- Check preferred DC list was copied if it existed
- Check widlelink configuration was copied if it existed (converted to symlinks)
- Check symlink config was copied over if it existed

3.11.3 Check Symlinks

```
cifs symlinks show -vserver <vserver>
```

3.11.4 Check Options (set advanced)

```
cifs options show -vserver <vserver>
```

3.11.5 Check Group Policy

```
cifs group-policy show –vserver <vserver>
```

3.11.6 Check Preferred DC List

```
cifs domain preferred-dc show –vserver <vserver>
```

3.11.7 Check Group Membership

```
local-group show-members -vserver <vserver>
```

Example

```
eg-si-clsn-e01::> local-group show-members -vserver si-mptest-01
  (vserver cifs users-and-groups local-group show-members)
Vserver        Group Name                  Members
-------------- --------------------------- ------------------------
si-mptest-01   BUILTIN\administrators       SI-MPTEST-01\administrator
                                           SI-MPTEST-01\root
                                           TLR\Domain Admins
                                           TEN\Domain Admins
                                           TEN\M-Storage-admins.G
                                           TEN\M-EaganServerAdmins
               BUILTIN\users               TLR\Domain Users
               SI-MPTEST-01\monitor        SI-MPTEST-01\monitoruser
                                           TLR\M-West-SiteScope_ServiceAccounts
9 entries were displayed.
```

3.11.8 Check Local Groups

```
local-group show -vserver <vserver>
```

Example

```
eg-si-clsn-e01::> local-group show -vserver si-mptest-01
  (vserver cifs users-and-groups local-group show)
Vserver        Group Name                      Description
-------------- ------------------------------- ----------------------------
si-mptest-01   BUILTIN\administrators          Members can fully administer the filer
si-mptest-01   BUILTIN\backup operators        Members can bypass file security to backup files
si-mptest-01   BUILTIN\power users             Members that can share directories
si-mptest-01   BUILTIN\users                   Ordinary Users
si-mptest-01   SI-MPTEST-01\compliance administrators
                                               Members can perform compliance operations
si-mptest-01   SI-MPTEST-01\monitor            use powerhell to alert users
6 entries were displayed.
```

3.11.9 Check Local Users

```
local-user  show -vserver <vserver>
```

Example

```
eg-si-clsn-e01::> local-user  show -vserver  si-mptest-01
  (vserver cifs users-and-groups local-user show)
Vserver      User Name                   Full Name            Description
------------ --------------------------- -------------------- -------------
si-mptest-01 SI-MPTEST-01\administrator                       Built-in account for administering
the filer
si-mptest-01 SI-MPTEST-01\monitoruser                         powershell user to monitor vfilers
si-mptest-01 SI-MPTEST-01\root                                Default vfiler root
3 entries were displayed.
```

3.11.10 Check Share Permissions and Path To Volume/Qtree

```
cifs share show -vserver <vserver>
```

Example

```
eg-si-clsn-e01::> cifs share show -vserver si-mptest-01
Vserver        Share         Path              Properties Comment  ACL
-------------- ------------- ----------------- ---------- -------- -----------
si-mptest-01   admin$        /                 browsable  -        -
si-mptest-01   c$            /                 oplocks    -        BUILTIN\Administrators / Full
Control
                                               browsable
                                               changenotify
si-mptest-01   ipc$          /                 browsable  -        -
si-mptest-01   mpqt01        /cb123_           browsable  -        everyone / Full Control
                             mptestvol01/      oplocks             TEN\uc136758 / Full Control
                             mpqt01            changenotify
si-mptest-01   mpshare01     /cb123_           browsable  -        everyone / Full Control
                             mptestvol01       oplocks             TEN\uc136758 / Full Control
                                               changenotify
5 entries were displayed. TLR\Domain Admins / Full Control
```

3.11.11 Export Policy Script

There is a script which can be run post migration to create volume export policies and also populate the default and volume export policy rules. The script arguments are shown below.

```
7-c_nfsexports.pl

Usage: ./7-c_nfsexports.pl --file <file name> --cb <CBEntry> --vserver <vserver name> --type <DB or
STD> --user <user name> --cluster <C-DOT clustername>
```

Example

The following example will create volume export policies and populate the rules in both the default policy and volume export policies. The 7-Mode exports file used is below:

```
#Auto-generated by setup Tue Aug 25 23:10:21 GMT 2015
/vol/si_nastest_01_root -sec=sys,rw,anon=0,nosuid
#/vol/si_nas_test01     -sec=sys,rw,nosuid
#/vol/Image1    -sec=sys,rw,nosuid
#/vol/nfstest01 -sec=sys,rw,nosuid
#/vol/nfstest02 -sec=sys,rw,nosuid
#/vol/test_7mtt_02      -sec=sys,rw,nosuid
#/vol/test_7mtt_01      -sec=sys,rw,nosuid
/vol/mptestvol01        -sec=sys,rw,nosuid
/vol/mptestvol01/mpqt01 -sec=sys,rw=10.220.177.29,root=10.220.177.29
```

You provide the cluster admin name/IP and the admin user. It is assumed you have SSH public key access.

```
./7-c_nfsexports.pl --file ./expfile --cb cb123 --vserver si-mptest-01 --type STD --user admin --
cluster 10.220.194.42

Extacting the data from supplied exports file.........
Extracting the hosts list by options(ro,rw,root)......
Bringing up the qtree hosts to volume.................
Eliminating the duplicate hosts at vol level.........
generating volume export policies........
Collect default and volume based exports: OUT ............
```

The script creates all of the objects on the cluster as shown below (note the CIFS rule added due to MP access):

Default Export Policy Rules

```
eg-si-clsn-e01::> export-policy rule show -vserver si-mptest-01 -policyname default
  (vserver export-policy rule show)
             Policy          Rule    Access   Client                RO
Vserver      Name            Index   Protocol Match                 Rule
------------ --------------- ------  -------- --------------------- ---------
si-mptest-01 default         1       any      10.220.177.29         sys
si-mptest-01 default         2       cifs     0.0.0.0/0             any
2 entries were displayed.
```

Volume Export Policy Rules

```
eg-si-clsn-e01::> export-policy rule show -vserver si-mptest-01 -policyname cb123_mptestvol01
  (vserver export-policy rule show)
             Policy          Rule    Access   Client                RO
Vserver      Name            Index   Protocol Match                 Rule
------------ --------------- ------  -------- --------------------- ---------
si-mptest-01 cb123_mptestvol01
                             1       any      10.220.177.29         sys
1 entries were displayed.
```

Volume Export Policies

```
eg-si-clsn-e01::> vol show -vserver si-mptest-01 -fields policy
  (volume show)
vserver      volume            policy
------------ ----------------- -----------------
si-mptest-01 cb123_mptestvol01 cb123_mptestvol01
si-mptest-01 si_mptest_01_root default
2 entries were displayed.
```

3.11.12 Volume UNIX Permissions

```
eg-si-clsn-e01::> vol modify -vserver si-mptest-01 -volume cb123_mptestvol01 -unix-permissions
rwxrwxrwx

  (volume modify)
```

3.11.13 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 snapshot autodelete show -vserver <vsname>

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

volume snapshot autodelete show -vserve <vsname>
```

3.12 QoS Policy Group Creation for Shared Filers

All shared filer volumes have a QoS policy set at 6000iops as shown below. Exceptions to this policy must be agreed by D&E management on a case by case basis.

3.12.1 Create QoS policy group and apply it at the volume level (create one QOS policy for each volume)

```
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-group
```

3.13 QoS Policy Group Creation For Dedicated Filers

All dedicated filer volumes have a QoS policy set at INF as shown below. This enables statistics to be collected but no limits are placed on the volume with regard to IOPS.

3.13.1 Create QoS policy group and apply it at the volume level (create one QOS policy for each volume)

```
qos policy-group create -policy-group <volname> -vserver <vsname> -max-throughput INF

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

qos policy-group show

volume show –vserver <vsname> -fields qos-policy-group
```

4 Snapvault Configuration

4.1 Cluster and Vserver Peering

4.1.1 Confirm that cluster peering has been enabled

```
cluster peer show
```

4.1.2 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
```

4.1.3 Confirm if vserver peering has been configured

```
vserver peer show
```

4.1.4 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
```

4.1.5 Accept the vserver peering on the source system

```
vserver peer accept -vserver <source_vserver> -peer-vserver <destination_vserver>
```

```
vserver peer show
```

4.2 SnapVault configuration

Volumes names in TR have ‘SNAP’ or ‘NOSNAP’ incorporated into them. SNAP volumes must have snapvault configured for disk based backups. NOSNAP volumes do NOT require backups.

4.2.1 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
```

4.2.2 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
```

4.2.3 Configure a snapmirror policy on the destination

```
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
```

4.2.1 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
```