NetApp Solution Deployment Guidelines

Thomson Reuters – Oracle on NetApp cDOT

Synopsis:	This document details the NetApp clustered Data ONTAP solution used for storage in Oracle environments at Thomson Reuters.

Authors: Michael Arndt (arndt@netapp.com)

Contributors: David Ng, Mitchell Vallone, Ken Zola, Ian Daniel

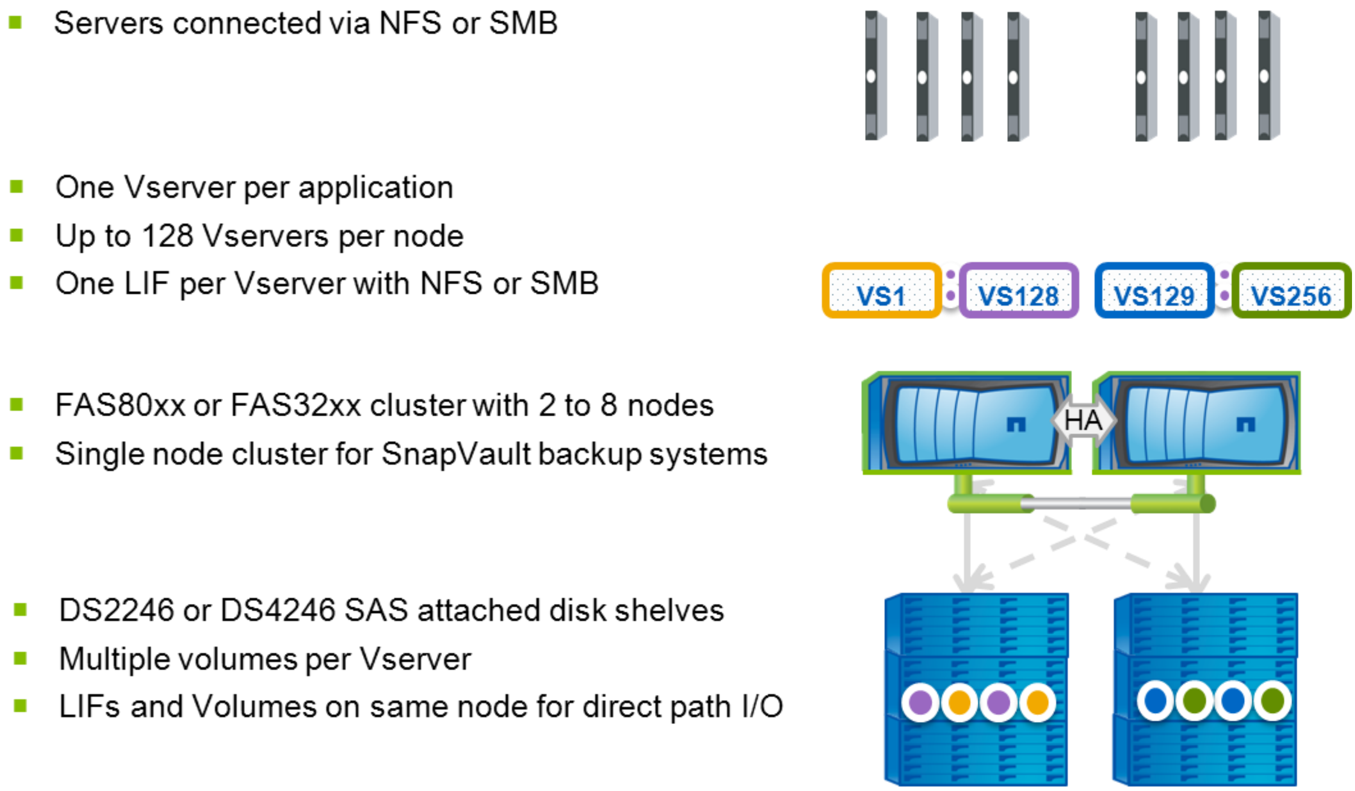
Document Version: V30
Date: May 2014

Contents

1 Introduction

1.1 Management Summary

This document details the NetApp clustered Data ONTAP (cDOT) solution used for Oracle environments at Thomson Reuters. The storage system configuration of Vservers, Networking, Volumes, and Storage Efficiency will be covered in detail. The following drawing gives a high level overview of the cDOT shared storage environment solution at Thomson Reuters.



- 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 Assumptions

It is assumed the person(s) reading this document are conversant with NetApp hardware and software. They will also be conversant with the Linux operating systems, NFS protocol, and database systems at a high level.

1.3 Change History

Ver	Date	Author	Key Changes
1	November 2013	Michael Arndt	Initial Version
2	November 2013	Michael Arndt	Updated archive log volume naming conventions and added recommendation for tcp_max_slot_table_entries.
3	November 2013	Michael Arndt	Add DNS configuration example.
4	November 2013	Michael Arndt	Added better examples of snapshot restore commands.
5	March 2014	Michael Arndt	Updated linux tuning, init.ora parameters, and Oracle patches required for DNFS environments.
6	May 2014	Michael Arndt	Updates to snapshot naming conventions.
	October 2014	David Ng	Update based on TR testing
19	December 2014	David Ng	Added restore command for backup/restore user
20	January 2015	David Ng	Review and update typos
24	Febuary 2015	David Ng	Added snapvault configuration
30	March 2015	David Ng	Added new snapsvault retention per Storage Architectures

			recomendation

1.4 Distribution List

Name	Role
Brett Truhler	Customer
Stewart Bird	Customer
Dan Dressel	Customer
Boris Belous	Customer
Mitchell Vallone	Reviewer
Michael Arndt	Reviewer
Ian Daniel	Reviewer
Kevin Atkins	Reviewer

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.
QoS	Quality of Service – introduced in cDOT 8.2 to provide workload monitoring and throughput rate limiting as desired.
WFA	OnCommand Workflow Automater – An automation framework application from NetApp, used for storage provisioning.

1.6 What is new in cDOT for Oracle environments at TR

While many concepts and configuration tasks remain identical in the NetApp cDOT storage environment for Oracle, as compared to the NetApp 7 Mode environment, a few things are different. The following gives a list of the most visible changes that the reader should be aware of:

- The path that is mounted from the NFS client changes in cDOT. While the NFS mountpoints for all 7 Mode systems start with */vol/*, this is no longer the case with cDOT. As such, it will be easy to determine if a NetApp system is running 7 Mode or cDOT by simply looking at the path to the volume being mounted. For example, this would be a path to a 7 Mode volume in a NFS mountpoint:

  <vFiler>:/vol/<volname>/<qtreename>

  In cDOT, the path would instead look like this:

  <Vserver>:/<volname>/<qtreename>

- Performing restores of single files in cDOT will be significantly faster than in 7 Mode, as the system uses a cloning technology that will complete the restore process in seconds, regardless of the file size. The SnapRestore licensing on a cDOT storage system allows for the use of this cloning technology during restore scenarios. A FlexClone license is therefore only required when making clones for the purposes of having additional copies of an object available, or for making a read/write copy of a snapshot.

- The method for creating snapshots on primary storage in the Oracle hot backup script changes, as compared to the process used by the Oracle hot backup scripts for 7 Mode. Section 6 provides example code for creating snapshots, removing old snapshots, and calculating SnapVault lag time on a cDOT system.

- Restores from the SnapVault secondary will be more easily performed, as cDOT uses a better integrated volume SnapVault process as compared to the process used by TR for 7 Mode.

2 NetApp Storage System Configuration

2.1 General configuration

The typical configuration for Oracle databases using NetApp storage within TR is to allocate 1 Vserver with 1 LIF per Oracle database. When configuring Vservers for use with Oracle databases, the following configuration options and limitations should be taken into consideration:

- The Oracle database servers must be able to access the Vserver via NFSv3 and SSH.
- While the Oracle database servers and the Vserver LIF do not need to reside on the same network subnet, the path should include a minimal number of network hops.
- Each Vserver will be configured with a local account, named *oracle*, used for communication via SSH between the Oracle server and the Vserver. The account should be created with a role that has access to the *volume snapshot* and *set* command directories.

2.2 Volume and Qtree layout

Each Oracle deployment will typically have 3 flexvols configured on a NetApp primary storage system, as show in the following table. The following table gives a high level description of the volumes and qtrees used in a typical LION configuration for TR.

Storage Volume	Storage Qtree	Description	Snap Reserve	SnapVault?
<cb#>_<app>_n01ora1_nosnap	n01oracluster1	RAC OCR/Vote (required if RAC is installed)	0%	No
	n01oradata1	Control, Temp, Online and Standby Redo logs		
	n01oraflash1	Flashback Recovery area if in use		
	n01oraadmin1	Admin area, does not require backup – ADR		
	n01oraggsdata	GoldenGate records, queue and trail files (required if Golden Gate is installed)		
	n01oraggsbin	GoldenGate software and configuration (required if Golden Gate is installed)		
<cb#>_<app>_s01ora1_snap	s01oradata1	Data and control files (required for SNAP)	20%	Yes
<cb#>_<app>_s01oraadm1_snap	s01oraadmin1	Admin area, spfile	20%	Yes

When provisioning volumes and qtrees for an Oracle configuration, the following should be noted:

- Sizing requirements will be provided by DBA team, based on their requirements and their standard sizing templates for LION configurations.
- The qtrees in the nosnap volume will have quotas configured, with the tree quota limit as determined by the sizing input given by the DBA team.
- The qtrees in the snap volumes will not have quotas configured, since there is only a single qtree in the volume. We will still create the qtree just to maintain a consistent layout as compared to the 7 mode implementation.

The follow configuration settings apply for each *_snap* volume, in order to implement snap autodelete:

- Set the *space-mgmt-try-first* volume setting to *snap_delete*
- Enable *volume snapshot autodelete*

2.3 Snap Reserve sizing and monitoring

For volumes on which snapshots will be taken, the Snap Reserve configuration listed in section 2.2 is 20%. A 20% snap reserve has shown to be adequate for most applications, without wasting space. This can be increased in the event that an application is consistently over-utilizing their Snap Reserve area and having too many snapshots autodeleted. Snap autodelete is used to keep the Snap Reserve area from overflowing into the active filesystem portion of the volume.

2.4 Snapshot backup configuration on primary storage

Snapshot creation for the s01ora1_snap volume on primary storage will be driven completely by scripts running on the Oracle server. These scripts will use SSH to run a *volume snapshot create* command while the database is in hot backup mode. In order to support the creation of snapshots that can be vaulted, the *snapmirror-label* argument must also be used when creating snapshots. By convention at TR, we will set the *snapmirror-label* to a value of *snapvault*, and all such snapshots will be vaulted to the secondary system.

The s01oraadm1_snap for each database volume does not get snapshots taken as part of the backup process, and instead will have snapshots created on primary storage as part of a schedule associated with a volume snapshot policy. Again, these snapshots will use a *snapmirror-label* of *snapvault* to allow them to be transferred to the SnapVault secondary system.

Examples of the snapshot and snapvault configuration are given in the *Clustered ONTAP provisioning CLI examples* section of this document. An example of a script that uses cDOT commands for snapshot creation, rotation, and snapvault lag time calculation is given in the *Oracle hot backup script example* section.

2.5 SnapVault backup configuration on secondary storage

The SnapVault relationship for volumes with Oracle databases on them will be initialized in the same way that all SnapVault relationships are configured within a cDOT system. By convention within the TR environment, they will be configured to vault all snapshots with a snapmirror-label of *snapvault*.

Note that the timing of the SnapVault replication updates is configured on the SnapVault secondary, and therefore snapshot creation via Oracle backup scripts should be configured to take place on primary storage prior to the replication update start time configured on the SnapVault secondary.

2.6 QoS configuration

In the TR shared storage environment, QoS policies with specific rate limits will be configured on each volume. One QoS policy group will be configured per volume, and the policy group will be named the same as the volume name.

For dedicated storage environments at TR, QoS policies should still be configured in the same manner as the shared environment, with the one difference being that the policy group can be set without a throughput limit. This is done in order to utilize the QoS latency statistics.

3 Oracle server configurations related to NetApp storage

3.1 Database file layout

Each Oracle database will use a number of NFS mountpoints to store their data. The following table gives a high level description of the standard NFS mountpoint layout and how it maps to the volume layout on the NetApp storage system. A more detailed document on the sizing and configuration for these mountpoints is available from the TR DBA team.

Mount Description	Mountpoint	Storage Volume	Storage Qtree
RAC OCR/Vote	/n01/oracluster1	<cb#>_<app>_n01ora1_nosnap	n01oracluster1
Control, Temp, Online and Standby Redo logs	/n01/oradata1		n01oradata1
Flashback Recovery area if in use	/n01/oraflash1		n01oraflash1
Admin area, does not require backup – ADR	/n01/oraadmin1		n01oraadmin1
GoldenGate report, trail & queue	/n01/oraggsdata		n01oraggsdata
GoldenGate software and configuration if used	/n01/oraggsbin		n01oraggsbin
Data and control files	/s01/oradata1	<cb#>_<app>_s01ora1_snap	s01oradata1
Admin area, requires backup – spfile	/s01/oraadmin1	<cb#>_<app>_s01oraadm1_snap	s01oraadmin1

In the event that additional volumes are required when using multiple instances of Oracle on the same Oracle database servers, a second set of mountpoints with a slightly modified naming convention (n02 and s02 instead of n01 and s01) is configured as follows:

Mount Description	Mountpoint	Storage Volume	Storage Qtree
Control, Temp, Online and Standby Redo logs	/n02/oradata1	<cb#>_<app>_n02ora1_nosnap	n02oradata1
Flashback Recovery area if in use	/n02/oraflash1		n02oraflash1
Admin area, does not required backup – ADR	/n02/oraadmin1		n02oraadmin1
Data and control files	/s02/oradata1	<cb#>_<app>_s02ora1_snap	s02oradata1
Admin area, requires backup – spfile	/s02/oraadmin1	<cb#>_<app>_s02oraadm1_snap	s02oraadmin1

3.2 Oracle archive log storage

The database file layout guidelines given above do not address the location of Oracle archive logs. Oracle archive logs will be written to a NFS mountpoint served by a different Vserver that resides on a dedicated cDOT log backup storage system. The dedicated cDOT log backup storage system will have one volume per Oracle instance with no qtrees being used, and it will be configured with post-process compression. The volume name will have _*<ret#>*_ in it, where *<ret#>* is the number of days that the logs are retained, with the possible values being 7, 14, 30, or 45.

In the event that this primary log backup storage is unavailable due to a planned or unplanned outage, Oracle switches to writing the archive logs to a 7 Mode NetApp NFS mountpoint. The 7 Mode NetApp storage is configured as a single thin provisioned volume per datacenter module named infra_nosnap, with each instance of Oracle having it's own qtree for archive log storage.

The following table describes the NFS mountpoints used by the Oracle server for achive log storage. These volumes should be created by using the WFA.

Mount Description	Mountpoint	Storage System	Storage Volume	Storage Qtree
Primary archive area	/n01/oraarch1	NetApp cDOT	<cb#>_<app>_<ret#>_n0<inst#>oraarch1_nosnap	
Alternate archive area	/n01/oraarch2	NetApp 7 Mode	infra_nosnap	<bu>_<app>_n01oraarch2

3.3 NFS mount options

NetApp and Oracle have well defined and jointly supported NFS mount options for Oracle single instance and Oracle RAC environments. The following Best Practices for Oracle Databases on NetApp Storage document on the NetApp support site (login required) documents these best practices:

http://www.netapp.com/us/media/tr-3633.pdf

Note that for Oracle RAC configurations, the “actimeo=0” NFS mount option is listed as being required for all Oracle mountpoints. While this is the published best practice by both NetApp and Oracle, we have seen within the TR environment that a large amount of NFS GETATTR and LOOKUP traffic is occasionally generated within the ADR location (/n01/oraadmin1). After extensive testing, and the relocation of the spfile to the /s01/oraadmin1 mountpoint, TR has determined that the actimeo=0 NFS mount option can be removed from the /n01/oraadmin1 mountpoint. This configuration is only in place for LIONv2 configurations.

This has shown a dramatic reduction in NFS operations on that mountpoint in some instances, and therefore this reduces the load significantly on shared storage systems hosting multiple Oracle databases. Any configuration not following the exact LIONv2 standard for the Oracle file layout should adhere to the recommendations in the KB article and use actime=0 on all mountpoints.

3.4 Linux kernel TCP tuning on the Oracle server

A number of TCP tunings are used in the Linux kernel of the Oracle server, in order to ensure the best possible performance. The following is a subset of the settings used in /etc/sysctl.conf on the Oracle server, as they are defined for the LIONv2 standard. The TR DBA and Platform management teams can provide the full list of settings based on a specific implementation, and whenever possible the TR standard and tested configurations should be used. This section is included in this document only to remind the reader that these types of Linux kernel settings are important in order to ensure the best possible performance when running Oracle over NFS.

```
# 10GigE Standard Network Tunables for TR
net.core.rmem_default = 16777216
net.core.rmem_max = 16777216
net.core.wmem_default = 16777216
net.core.wmem_max = 16777216
net.ipv4.tcp_wmem = 16777216 16777216 16777216
net.ipv4.tcp_rmem = 16777216 16777216 16777216
net.core.netdev_max_backlog = 300000

# Increase NFS over TCP parallelism
sunrpc.tcp_slot_table_entries = 128
sunrpc.tcp_max_slot_table_entries = 128
```

4 Oracle backup and recovery

The Oracle backup and recovery procedures documented here are focused on the use of NetApp snapshots for Oracle datafile backup and recovery.

4.1 Oracle backup

Backups are initiated by a shell script, scheduled in cron, from the Oracle server. This shell script, amongst other tasks, will put the Oracle tablespaces in hot backup mode and then run a *volume snapshot create* command via SSH on the Vserver hosting it's *s01ora1_snap* volume. This requires SSH publickey authentication to be properly configured between the Oracle server and the Vserver hosting it's volumes. Each DBA group within TR manages it's own shell script for doing Oracle backups, but the method by which the snapshots are taken is identical in all scripts.

4.2 Oracle restore scenarios

4.2.1 Restoring a single datafile from primary snapshot backups

There are two methods by which restores of single files can be performed from snapshots on primary storage. The first option is to use a simple *cp* command from the Oracle server to copy data from a snapshot directory back to the active filesystem. To see the snapshots available on primary storage, *cd* into the directory where the restore is required. Then use *cd .snapshot* and *ls –lu* to see the snapshots that are available. Once the snapshot path to the file to be restored has been identified, it can be copied back to the fully qualified path to the active filesystem. For example:

```
cp /s01/oradata1/.snapshot/<dir>/<snapshot_name>/<filename> /s01/oradata1/<dir>/<filename>
```

The second option is to use the single file snap restore capabilities on the NetApp storage system to perform the restore. You can use the *volume snapshot show* command to determine which snapshot you want to use for the restore, or you can use the *ls –lu* command as described above to view the available snapshots. The single file snap restore and snapshot related commands can be run on the NetApp storage controller via a SSH connection from the Oracle server, and multiple files can be restored in parallel by issuing multiple commands via SSH. For example, the syntax is as follows:

```
ssh <Vserver> volume snapshot show –volume <volume_name>

ssh <Vserver> volume snapshot restore-file –volume <volume_name> –snapshot <snapshot_name>
-path </vol/volname/path/to/filename>
```

In addition, the following examples show the full commands from a POC environment:

```
ssh test-wfa-c0094 volume snapshot show –volume wfa94_test35_s01ora1_snap

ssh test-wfa-c0094 volume snapshot restore-file –volume wfa94_test35_s01ora1_snap  –snapshot
oracle_hotbackup_20131121_ 1654 -path
/vol/wfa94_test35_s01ora1_snap/s01oradata1/POC036A/datafile/o1_mf_users_98tbxsns_.dbf
```

The use of the single file snap restore command will be significantly faster than a simple client based "cp" command to restore files from snapshots, since single file snap restores within cDOT are actually performed by cloning the file from a snapshot. This allows for single file snap restores in cDOT to complete within seconds, regardless of the size of the file being restored.

4.2.2 Restoring all datafiles in a volume from primary snapshot backups

In some use cases, it is necessary to restore all files in a given volume back to a previous point in time. When this is required, NetApp storage controllers have the ability to perform a volume snap restore operation. While this is similar in concept to the single file snaprestore, it has some very important differences:

• Using a volume snap restore can result in snapshot backups being removed from the volume. If a volume snap restore is used to restore to a snapshot that is older than the most recently created snapshot, then all of the snapshots that are newer than the snapshot being used for the restore will be removed. This is because a volume snap restore reverts the entire volume, including snapshots of the volume, back to the state as it existed when the snapshot being used for the restore was created.

An example of the syntax for performing a volume snap restore is provided here:

```
ssh <Vserver> “set advanced; volume snapshot restore –volume <volume_name> –snapshot
<snapshot_name>“
```

In addition, the following example shows the full command from a POC environment:

```
ssh test-wfa-c0094 “set advanced; volume snapshot restore –volume wfa94_test35_s01ora1_snap –
snapshot oracle_hotbackup_20131121_ 1654“
```

The SnapVault backup relationship to secondary storage may need to be re-initialized after a full snapshot restore.

4.2.3 Restore from Secondary snapshot backups

In the event that the snapshot backups required for the restore are no longer available on primary storage, the restore must be performed from secondary storage. Again, there are two ways in which this restore can be accomplished.

The first option is that the SnapVault secondary volume can be exported to the Oracle server, and it can be mounted via NFS on the server where the restore is required. This will require that the Oracle DBA make a request to the storage support team for the NFS export of the SnapVault secondary volume to be configured. The Oracle DBA can then use a simple copy operation, similar to what was described in section 4.2.1, to copy data from a snapshot on secondary storage back to the active filesystem on primary storage. The advantage to using this method is that the Oracle DBA has all the secondary snapshots at their disposal for use in the restore process. This can be useful if the DBA is not sure which version of a given file will be required, as they can quickly change to using a different snapshot for their restore process.

The second option is that the Oracle DBA can request that a SnapVault restore be performed to revert the entire contents of the primary storage volume(s) to a point in time from a previous backup. If a SnapVault restore is used to restore to a snapshot that is older than the most recently created snapshot, then all of the snapshots that are newer than the snapshot being used for the restore will be removed. This is because the SnapVault restore reverts the entire volume, including snapshots of the volume, back to the state as it existed when the snapshot being used for the restore was created.

An example of performing a volume snapvault restore is provided here:

```
snapmirror restore -destination-path <Primary_Vserver>:<Primary_Volume> -source-path
<Secondary_Vserver>:<Secondary_Volume> -source-snapshot <snapshot_name>
```

In addition, the following example shows the full command from a POC environment:

```
snapmirror restore -destination-path test-wfa-c0094:wfa94_test35_s01ora1_snap -source-path lab-
aibkp-001:sv_14_wfa94_test35_s01ora1_snap -source-snapshot oracle_hotbackup_20131121_1654
```

4.2.4 Partial tablespace restores from snapshot backups

In some cases, only a small portion of a tablespace needs to be restored from a snapshot backup copy. Examples of this use case would be having a single table, or a single row in a table, that needs to be restored. In these cases, a snapshot of the SnapVault secondary volume can be cloned on the secondary controller. This clone is essentially a writable copy of a snapshot, but it only requires storage for blocks that are changed, and therefore it can be created very quickly (typically 10 seconds or less) regardless of the dataset size. This clone can then be exported via NFS to an Oracle restore server that would be used to bring up a version of the database that is used for restore purposes. While this method is not widely used within TR, the concept is documented here so that it can be considered for future restore scenarios.

5 Clustered ONTAP provisioning CLI examples

While WFA is meant to be used for storage provisioning in the Oracle environment, it may be useful to know the exact commands that would be used in the event that provisioning needed to be done manually for any reason.

5.1 Vserver and LIF creation

5.1.1 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 C.UTF-8
```

```
vserver show
```

5.1.2 Create LIF with default route and failover group

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

5.2 DNS configuration

5.2.1 Setup DNS on a Vserver

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

```
vserver services dns show
```

5.3 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>
```

5.4 Oracle account setup

5.4.1 Oracle role, user, and SSH publickey configuration (ssh keys are located in DFM server ‘/filers/admin/source/logical’)

```
security login role create -role oracle -cmddirname "volume snapshot" -access all -vserver <vsname>

security login role create -role oracle -cmddirname "set" -access all -vserver <vsname>

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

security login role create -role oracle -cmddirname "job show" -access readonly -vserver <vsname>

security login role create -role oracle -cmddirname "df" -access readonly -vserver <vsname>

security login role create -role oracle -cmddirname "snapmirror list-destinations" -access readonly –vserver <vsname>

security login create -username oracle -application ssh -authmethod publickey -role oracle -vserver <vsname>

security login publickey create -username oracle -vserver <vsname>  -publickey "<ssh-dss pub_key_string>"
```

5.5 NFS and CIFS configuration

5.5.1 Enable NFSv3

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

vserver nfs show
```

5.6 Primary job schedule and snapshot policy configuration

5.6.1 Create job schedule and snapshot policy (only execute for OraAdmin volume):

```
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 <volume_name>

job schedule cron show -name <vol_name>

volume snapshot policy show –vserver <vsname>
```

5.7 Volume creation

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

```
vserver export-policy create –vserver <vsname> –policyname <volume_name>
```

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

```
vserver export-policy rule create -vserver <vsname> -policyname default

-clientmatch <nfsclient> -rorule sys -rwrule sys -superuser sys
```

5.7.3 Create 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
```

5.7.4 Create primary NOSNAP volume

```
volume create -vserver <vsname> -volume <nosnap_volname> -aggregate <aggrname> -size <size> -policy <volume_name> -snapshot-policy none -junction-path /<nosnap_volname> -security-style unix –space-guarantee none –percent-snapshot-space 0 –language C.UTF-8

volume show –vserver <vsname>

vserver export-policy rule show
```

5.7.5 Create primary Oraadmin SNAP volume

```
volume create -vserver <vsname> -volume <oraadm_volname> -aggregate <aggrname> -size <size> -policy <volume_name> -snapshot-policy daily<hour> -junction-path /<oraadm_volname> -security-style unix –space-guarantee none –percent-snapshot-space 20 –language C.UTF-8
```

5.7.6 Create primary Oradata SNAP volume (this volume is only required if SNAP was requested on Oradata)

```
volume create -vserver <vsname> -volume <ora1_volname> -aggregate <aggrname> -size <size> -policy <volume_name> -snapshot-policy none -junction-path /<ora1_volname> -security-style unix –space-guarantee none –percent-snapshot-space 20 –language C.UTF-8
```

5.7.7 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 -vserver <vsname>
```

5.7.8 Create primary qtrees with quotas (repeat command below for each required qtree. Section 3.1 can be used as reference)

```
volume qtree create -vserver <vsname> -volume <volname> -qtree <qtname> -security-style unix
volume quota policy rule create -vserver <vsname> -policy-name default -volume <nosnap_volname> -type tree -target <qtname> -disk-limit <XXXg>
```

5.7.9 Enable the quotas (repeat step for each volume>

```
volume quota on -vserver <vsname> -volume <volname>
```

5.8 QoS policy group creation

5.8.1 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
```

6 Snapvault Configuration

6.1 Cluster and Vserver Peering

6.1.1 Confirm that cluster peering has been enabled

```
cluster peer show
```

6.1.2 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
```

6.1.3 Confirm if vserver peering has been configured

```
vserver peer show
```

6.1.4 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
```

6.1.5 Accept the vserver peering on the source system

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

6.2 SnapVault configuration

There are two data protection configurations for LION: SNAP & NOSNAP. The ‘oradata’ and ‘oraadmin’ volume are vaulted in a SNAP configuration. Only the ‘oraadmin’ volume is vaulted in a NOSNAP configuration. Hence, the number of volumes you execute commands for may vary based on configuration type.

6.2.1 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 C.UTF-8 -type DP

volume show
```

6.2.2 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
```

6.2.3 Configure a snapmirror policy on the destination (execute these command for oraadmin & oradata)

- **7 day retention will have a snapshot count of 14 on the secondary**
- **14 day retention will have a snapshot count of 28 on the secondary**
- **30 day retention will have a snapshot count of 60 on the secondary**
- **45 day retention will have a snapshot count of 90 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
```

6.2.1 Initialize SnapVault relationship on the destination (execute these command for oraadmin & oradata)

```
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
```