Technical Report

Element Software for Oracle Configuration Guide

For SolidFire and NetApp HCI

Bobby Oommen, NetApp
August 2020 | TR-4768

NetApp®

TABLE OF CONTENTS

1 Introduction

1.1 Oracle Considerations

This document describes how to configure Oracle and NetApp Element software on NetApp SolidFire storage arrays and NetApp HCI in accordance with NetApp recommended best practices. Element Software on NetApp HCI and SolidFire arrays can support a wide range of database application use cases, such as database consolidation, dynamic resource allocation for development and testing environments, and integration of cloud infrastructure.

By leveraging the per-volume QoS of Element, you can be assured that individual databases will maintain sufficient I/O throughput without being affected by other workloads on the storage cluster. For more in depth information on Element Software QoS, refer to TR-4644: NetApp SolidFire Quality of Service (QoS) and TR-4632: NetApp HCI QoS and Mixed Workloads.

The snapshot capabilities of Element allow you to have point-in-time backups of the active file system or storage volume. You can use application-consistent snapshot copies for rapid recovery of corrupted datasets and to create space-efficient copies of datasets for development and testing. By using group snapshot copies, the multiple volumes for the database will be fully consistent. For more information on Element Software data protection refer to TR-4641: NetApp HCI Data Protection.

There is no restriction on running single Oracle or Oracle Real Application Clusters (RAC) instances on Element OS. However, you should also research other NetApp products if you want to achieve consistent submillisecond and high-bandwidth I/O performance. Oracle Licensing with NetApp HCI

1.2 CPU Optimization with NetApp HCI

The use of dedicated compute and dedicated storage servers is a key differentiator with NetApp HCI because it means that core-licensed products do not run on storage server CPUs. As a result, you can reduce the number of cores that must be licensed for products such as Oracle Database and can simplify software management and auditing.

The NetApp HCI architecture is also more efficient from a licensing and performance point of view because cores that are licensed for Oracle are not given the task of storage work. The CPU work that is required to present and to maintain a LUN, including features such as compression and deduplication, is isolated to a different system. It therefore does not create a “NetApp HCI tax” on the compute hypervisor, including its cores that were licensed for Oracle work.

1.3 Core Right-Sizing

The processing capabilities of CPUs have increased much faster than the processing demands of most database workloads. Sometimes databases are limited by CPU work, but it is generally a result of the processing limits of a single core and is not a limitation of the CPU. The result is an increasing number of idle cores on database servers that still must be licensed for the Oracle Database software. This underutilization of CPU resources is a waste of capital expenditure, not only in terms of licensing costs, but also in terms of the cost of the server itself, heat output, and so on.

For information NetApp HCI platform specifications, refer to the DS-3881: NetApp HCI Datasheet.

Oracle licensing requirements can be complicated, but as a rule, all cores in which the software product can run without deliberate user intervention must be properly licensed. Virtualization adds requirements because of the native clustering capabilities. There is no requirement to license all ESX clusters under a single VMware vCenter Server, although the ability to migrate workloads between clusters does increase the chance of user error that leads to a license violation. A more common approach is to fully license a particular ESX cluster for core-licensed Oracle products. This approach reduces the risk of user error in VM placement while avoiding the licensing of unnecessary cores. All nodes are then available to provide high-availability (HA) services.

When it is not feasible to license all the cores, such as a large single ESX cluster, VMware affinity rules are often used to segment the cluster. For example, two out of six ESX nodes might be dedicated for Oracle work, and VMware affinity rules can prevent the software from running elsewhere. You must verify that new databases are properly restricted to the desired nodes. Finally, you can use VMware policies and affinity rules to limit the way that running database instances are tied to specific CPU cores. No controlling Oracle documentation currently exists for Oracle virtualization license policies. The recommended option is to reduce the number of cores that you deploy in a single server so that servers can be fully licensed wherever possible.

Next, by using the previously outlined guidelines, you explain your intended deployment of Oracle products on the NetApp HCI system to your Oracle account team, including the number of cores you are expected to license. If the Oracle account team expresses any concerns, ask them to clarify the policies with documented, binding authority that covers your scenario.

2 Storage Configuration

The configuration that is described in this document is for an Oracle database that uses an Oracle Automatic Storage Management (ASM) layout. You can also use a logical volume manager (LVM) configuration on Linux to configure the Oracle application. Element supports presentation of the storage in a 4K sector size (native mode) and in a traditional 512-byte sector size (512e). Provided that there is no partition misalignment at the host level, there is no performance effect from choosing emulation mode.

For the database layout, follow one of the storage configurations:

- iSCSI LUNs that are managed by the iSCSI initiator on the VM, not on the hypervisor
- Separate datastore and storage LUNs for Oracle data files, redo logs, and archival logs

To get the following benefits, you should avoid the use of datastores for Oracle files:

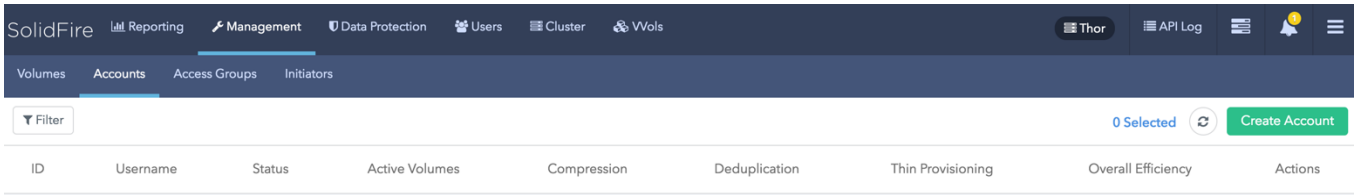
- **Transparency.** When a guest VM owns the file systems, it is easier for you to identify the source of the file systems for your data.
- **Manageability.** When a guest VM owns the file systems, manageability of provisioning, monitoring, and data protection across the environment becomes easier.
- **Portability.** When a VM owns its file systems, the process of moving an Oracle environment becomes simpler. File systems can easily be moved between virtualized and nonvirtualized guests and to other hypervisors.

  Note: NetApp strongly recommends that you use QoS policies to set the IOPS characteristics when you provision the volumes for the Oracle database. The use of QoS policies enables better manageability of IOPS settings at the volume level.

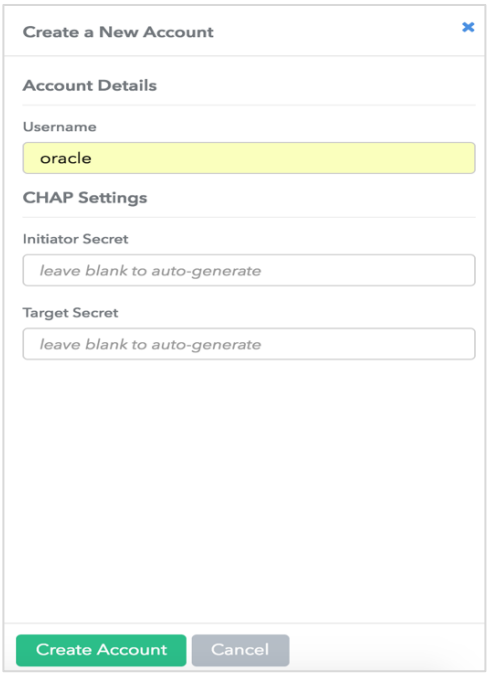
2.1 Create an Account

To create an account, complete the following steps:

1. Log in to the NetApp Element software UI.
2. Select Management > Accounts. The Account List window opens.



3. Click Create Account. The Create a New Account window opens.



4. Enter a user name.
5. In the CHAP Settings section, fill in the following fields:
   - Initiator secret for CHAP node session authentication
   - Target secret for CHAP node session authentication

   Note: Leave the credentials field blank if you want the passwords to be generated automatically.
6. Click Create Account.

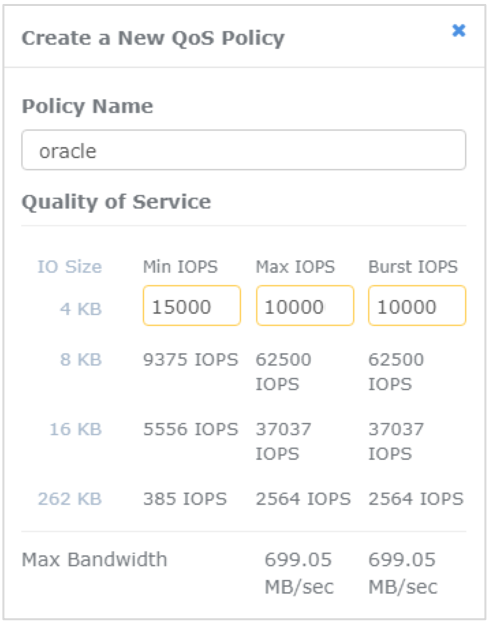
   Note: If an account with the same name exists, an error message will appear.

2.2 Create a QoS Policy

To create a QoS policy, complete the following steps:

1. Log in to the NetApp SolidFire Element UI.
2. Select Management > QoS Policies. QoS policy window opens.
3. Click Create QoS Policy.
4. Enter the QoS policies as required.

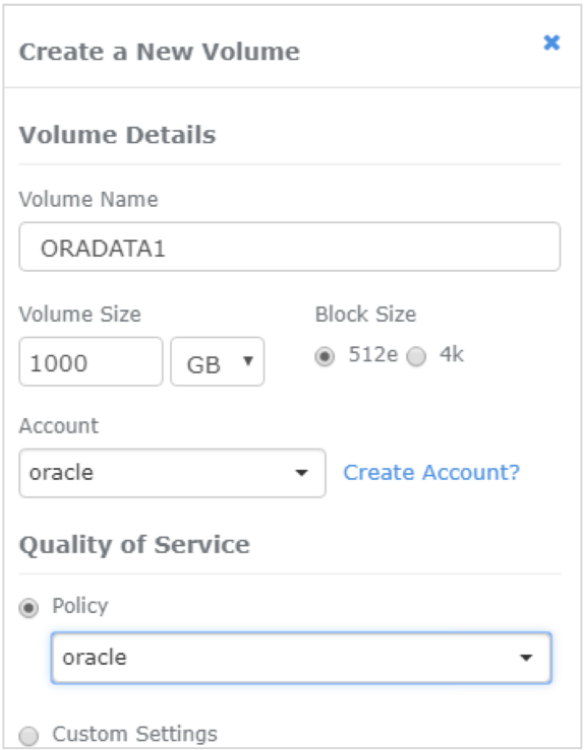
   For example: minimum 5K, maximum 100K, burst 100K. A proactive monitoring of the systems is performed through NetApp active IQ analytics; there are QoS recommendations for each volume.



2.3 Create a Volume

To create a volume, complete the following steps:

1. Log in to the Element UI.
2. Select Management > Volumes. The Volumes List window opens.
3. Click Create Volume. The Create a New Volume window opens.



4. Enter the volume name (1 to 64 characters in length). For example, provide the name as `ORADATA1`.

5. Enter the size of the volume.
6. Click the Account drop-down list and select the account that should have access to the volume. In this case, select oracle.
7. In Quality of Service options, select Policy and select the `oracle` policy created previously.
8. Click Create Volume.
9. Repeat steps 1 through 7 for all the remaining volumes (CRS1, CRS2, CRS3, ORADATA2, ORADATA3, and ORALOG1).

2.4 Create Volume Access Groups

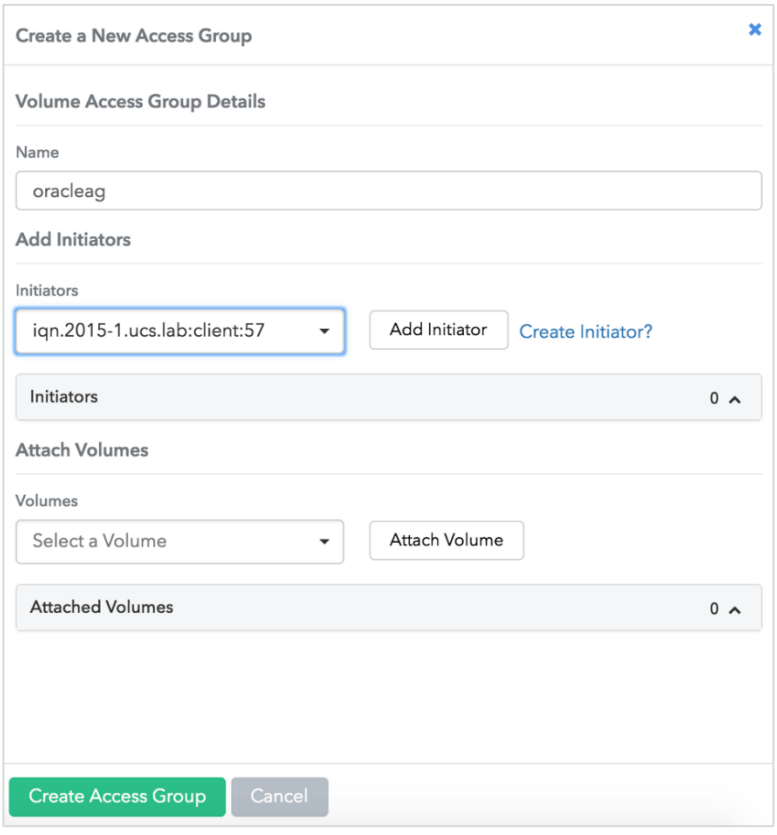
Volume access groups limit connectivity from designated host servers based on a unique identifier, whereas CHAP authentication uses secret keys for unidirectional or bidirectional authentication. In this document, initiator iSCSI qualified names (IQNs) are used to access the volumes.

Volume access groups have the following system limits:

- They can have a maximum of 64 IQNs.
- An IQN can belong to only one access group.
- A single volume can belong to a maximum of four access groups.

To create volume access groups, complete the following steps:

1. Log in to the Element.
2. Select Management > Access Groups. The Access Group window opens.
3. Click Create Access Group. The Create a New Access Group window opens.

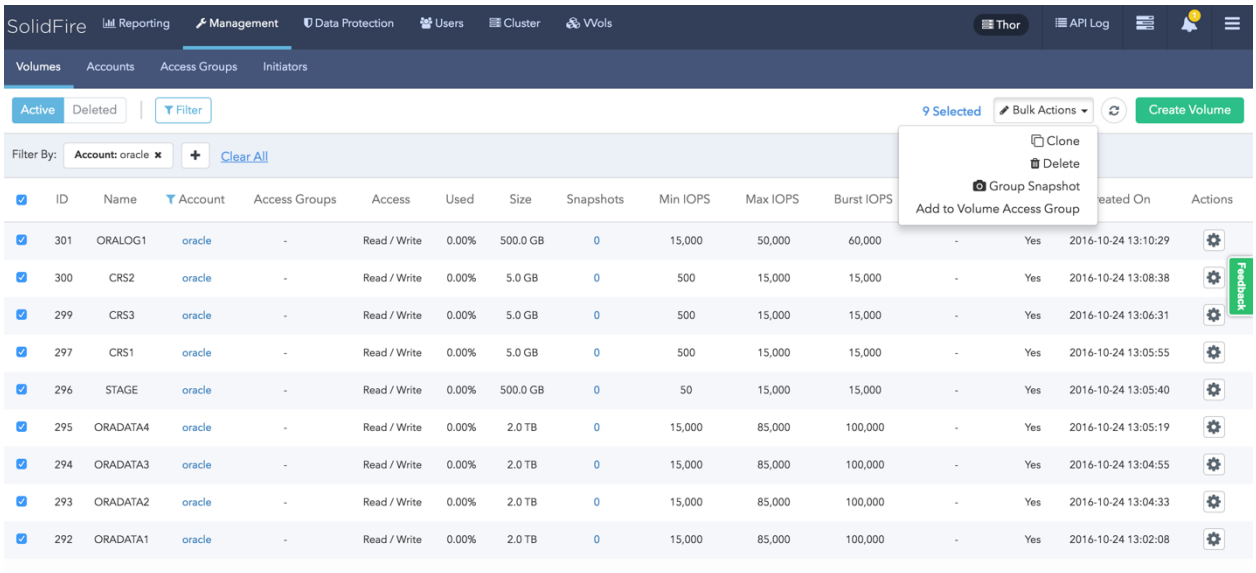


4. Enter a name for the volume access group.

5. Select the IQN from the initiator drop-down list or click Create Initiator.

   Note: Multiple IQNs are listed for Oracle RAC clusters, depending on the number of nodes.

6. Click Create Access Group.
7. Add the volumes to the access group by selecting Management > Volumes.
8. Select the checkbox to the left of each volume.
9. Near the Create Volume button, click the Bulk Actions drop-down list.
10. Select Add to Volume Access Group.



11. Scroll to the bottom and click Add to Volume Access Group. The Add to Volume Access Group window opens.
12. Select the previously created volume access group from the drop-down list.
13. Click Add to join the selected volumes to the target group.

The Oracle volumes are now listed as part of the selected volume access group. They are now ready for presentation to the host operating system after the host identifier is allowed into the volume access group configuration.

Note: For this configuration, four SolidFire volumes were chosen to distribute data across all four volumes in the ASM disk group. For a web-scale deployment, with hundreds of databases, NetApp recommends having just one volume for data for each individual database and that you control performance with the QoS settings.

3 Operating System Configuration

Before you proceed, follow the recommendations in TR-4639: Element Software Linux Configuration Guide to configure the operating system. These recommendations apply to Debian, SUSE, and Fedora based Linux distributions. This report assumes that a default installation of a software development workstation exists. You can use alternate distributions if they are fully compatible with the Oracle grid infrastructure and with Oracle Database software.

3.1 Add Packages

After you install the base operating system, you must update it to meet Oracle grid infrastructure and Oracle Database installation requirements. For further information, see the Oracle documentation and the release requirements, specifically the section “Install Prerequisite Packages.”

3.2 Update Kernel Parameters

Update the kernel parameters for your host operating system to the following values:

```
net.ipv4.ip_local_port_range = 9000 65500
net.core.rmem_default = 4194304
net.core.rmem_max = 16777216
net.core.wmem_default = 262144
net.core.wmem_max = 16777216
net.ipv4.ipfrag_high_thresh = 524288
net.ipv4.ipfrag_low_thresh = 393216
net.ipv4.tcp_rmem = 4096 524288 16777216
net.ipv4.tcp_wmem = 4096 524288 16777216
net.ipv4.tcp_window_scaling = 1
net.core.optmem_max = 524287
net.core.netdev_max_backlog = 2500
net.ipv4.tcp_mem = 16384 16384 16384
fs.aio-max-nr = 1048576
net.ipv4.tcp_no_metrics_save = 1
net.ipv4.tcp_moderate_rcvbuf = 0
vm.min_free_kbytes=262144
vm.swappiness=10
```

3.3 Optimize Network Performance

Consider the following guidelines for optimal network performance:

- Enable jumbo frames for all data network interfaces.
- The RAC interconnect should be configured with a different subnet than the RAC virtual IP address (VIP address) so that cluster interconnect traffic is fully isolated.
- Use separate virtual LANs (VLANs) for the management and data traffic.
- Add two virtual network interface cards (vNICs) for data traffic.

3.4 Set User Limits

Oracle recommends that you set the user limits to an optimal number because user limits affect application performance. For this solution, the following user limits were applied for both the `grid` and the `oracle` user. The same settings were applied on all RAC nodes. See the Oracle documentation for any updates to the following settings:

```
grid soft nproc 2047
grid hard nproc 16384
grid soft nofile 1024
grid hard nofile 65536
oracle soft nproc 2047
oracle hard nproc 16384
oracle soft nofile 1024
oracle hard nofile 65536
```

3.5 Set Permissions

Before the Oracle installation, you should set appropriate permissions so that Oracle can access the underlying devices on the NetApp HCI storage. You can set the device permissions on multipath devices by creating an `udev rule` file that allows the owner of the Oracle Database software to access the devices.

4 Oracle Configuration

4.1 Install Prerequisite Packages

NetApp recommends that you run the `runcluvfy.sh` script that is part of the Oracle installation package under the `grid` directory. This script thoroughly verifies all the required packages for each RAC node. You can run the script from the first RAC node, and it validates all the other nodes that are part of the cluster. The script can be executed as follows and is available in the `installer` directory of the grid installation software:

```
./runcluvfy.sh stage -pre crsinst -n rac1,rac2 -fixup -verbose -asm -asmdev
/dev/mapper/crs1,/dev/mapper/crs2,/dev/mapper/crs3
```

4.2 Configure Oracle ASM

The storage nodes automatically distribute and protect Oracle Database data across all nodes in the NetApp HCI cluster. For optimal distribution of data, use ASM to stripe data over all the storage volumes. This implementation helps confirm that all nodes can process Oracle writes and that Oracle Database I/O requests are uniformly distributed over all the nodes. As your capacity and performance requirements increase, you can dynamically create and add storage volumes to Oracle ASM disk groups.

If the overall throughput requirement of the database goes beyond 600MBps, NetApp recommends that you create more than one storage volume. You should also configure the ASM software to use a large allocation unit (64MB). The larger allocation unit reduces the amount of metadata and metadata updates that ASM requires to support a given amount of storage.

The storage nodes provide complete fault isolation through a comprehensive shared-nothing architecture. Therefore, ASM mirroring within a single cluster is not appropriate. For extreme fault tolerance, ASM mirroring can be used between clusters.

Note: ASMLib is a requirement on Linux when you use a 4KB native volume. Any volumes that you create with the default 512e are accessible by Oracle ASM.

4.3 Configure ASM Library

Oracle ASMLib simplifies storage deployment and management for Linux OS. Before you assign any LUN or volume to ASMLib, you must set the parameter `ORACLEASM_USE_LOGICAL_ BLOCK_SIZE` to `true`.

5 Microsoft Windows Configuration

Follow the recommendations in TR-4643: Element Software Windows Configuration Guide. The Windows OS automatically aligns disk partitions to storage sector boundaries. No specific tuning of the partition table layout or device queue depth settings is required with Windows on NetApp HCI. To configure Microsoft Windows, complete the following tasks:

1. Enable jumbo frames on the network interface cards (NICs).
2. To identify storage devices, enable Microsoft Multipath I/O (MPIO) and configure the Microsoft device-specific module (DSM).
3. Configure at least four iSCSI sessions per storage device.

6 Backup and Recovery Using Storage Snapshot Copies

You can take point-in-time (PiT) snapshots in Element for the volumes that are part of the Oracle Database. The application-consistent snapshots can be used to do database recovery in the event of

data corruption or media failure. SolidFire supports having multiple volumes for the database, and all volumes that are part of the database have the same consistency point during the group snapshot.

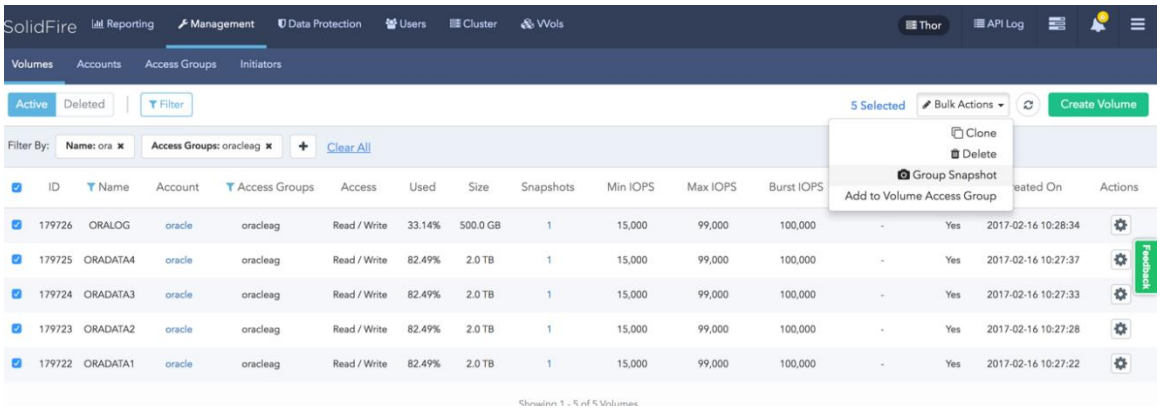
6.1 Create Snapshots (Backup)

To create backup snapshots, complete the following steps:

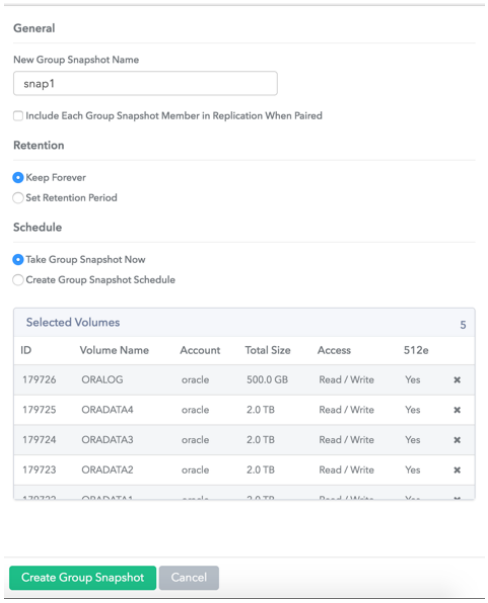
1. Log in to the Oracle instance. To put the database into backup mode, run the following commands:

```
alter system archive log current;
alter database begin backup;
```

2. Log in to the Element UI.
3. Select Management > Volumes. The Volumes List window opens.



4. Select the volumes that are part of the database.
5. Select Bulk Actions > Group Snapshot.



6. In the Create Group Snapshot window, enter a name for the snapshot (`Snap1` in this case).
7. Set the desired retention time.
8. Select Take Group Snapshot Now or select Create Group Snapshot Schedule.
9. Scroll to the bottom and click Create Group Snapshot.

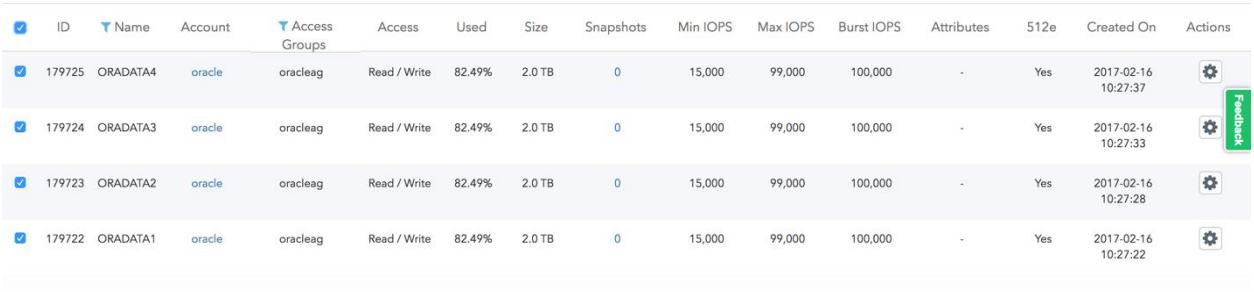
10. Take the database out of backup mode.

```
alter database end backup;
```

6.2 Restore Snapshots (Recovery)

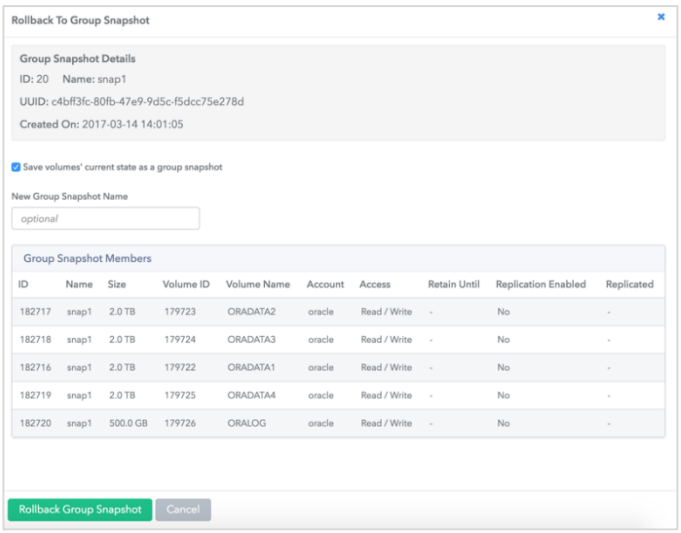
Database recovery can be performed by reverting the volumes on the SolidFire array using a snapshot. To recover the database, complete the following steps:

1. Log in to the Oracle Database server, stop the Oracle instance, and unmount the file systems that are part of the database. If the database is provisioned using ASM, stop the ASM instance.
2. Log in to the Element UI.
3. Select Data Protection > Group Snapshots. The Group Snapshot list opens.



ID	Name	Account	Access Groups	Access	Used	Size	Snapshots	Min IOPS	Max IOPS	Burst IOPS	Attributes	512e	Created On	Actions
179725	ORADATA4	oracle	oracleag	Read / Write	82.49%	2.0 TB	0	15,000	99,000	100,000	-	Yes	2017-02-16 10:27:37	
179724	ORADATA3	oracle	oracleag	Read / Write	82.49%	2.0 TB	0	15,000	99,000	100,000	-	Yes	2017-02-16 10:27:33	
179723	ORADATA2	oracle	oracleag	Read / Write	82.49%	2.0 TB	0	15,000	99,000	100,000	-	Yes	2017-02-16 10:27:28	
179722	ORADATA1	oracle	oracleag	Read / Write	82.49%	2.0 TB	0	15,000	99,000	100,000	-	Yes	2017-02-16 10:27:22	

4. Select the volumes that are part of the database.
5. Select Bulk Actions > Group Snapshot.
6. Click Actions.
7. Select Rollback Volumes to Group Snapshot. The Rollback to Group Snapshot window opens.



8. Click Rollback Group Snapshot.
9. After the volume is reverted successfully, log in to the Oracle instance.
10. Rescan the iSCSI devices.
11. Mount the file systems.
12. If the database is provisioned using ASM, start the ASM instance.
13. Log in to the Oracle instance and run these commands:

```
startup mount;
recover database;
alter database open;
```

7 RMAN Merge

RMAN merged incremental backups can reduce the time for Oracle Database recovery and are suitable primarily for disk-based backup and recovery. This method is widely used by database administrators. As part of the RMAN setup, a level 0 (full image) copy is created. Afterward, the subsequent RMAN runs and creates a level 1 incremental backup of the data file by using the system change number (SCN) as a reference. RMAN then applies all level 1 backups taken since the last backup to the image. The RMAN process uses a tag to link the incremental backups to the image copy. The configuration for this document is done with level 0 and incremental backups using two different locations on the RMAN target file system.

The target file system of the RMAN dump is created on the SolidFire array and is mapped to the database server with permission set so that an Oracle user can perform reads and writes. Four SolidFire volumes were used for this configuration, and the QoS settings were configured to meet the appropriate throughput requirements. On the Linux host, LVM was used to stripe data across multiple volumes.

7.1 Enable Block Change Tracking

Enabling the block change tracking feature improves the performance of incremental backups by recording changed blocks in the block change tracking file. During a backup operation, RMAN uses this file to identify the changed blocks that need to be backed up instead of scanning all data blocks to identify which blocks have changed. To enable block change tracking, connect to the RMAN target database instance and run the following commands:

```
ALTER SYSTEM SET DB_CREATE_FILE_DEST = '+ORADATA'; #The destination of the file changes depending
on the your setup
ALTER DATABASE ENABLE BLOCK CHANGE TRACKING;
```

7.2 Create RMAN Incremental

To perform the RMAN merge process incorporating SolidFire snapshots, complete the following steps:

1. Set the RMAN configuration parameters for the level 0 image.

```
CONFIGURE DEFAULT DEVICE TYPE TO DISK;
CONFIGURE CONTROLFILE AUTOBACKUP ON;
CONFIGURE BACKUP OPTIMIZATION ON;
CONFIGURE CONTROLFILE AUTOBACKUP FORMAT FOR DEVICE TYPE DISK TO
'/rmanfs/controlfile/control.%F.ctl';
CONFIGURE DEVICE TYPE DISK PARALLELISM 8 BACKUP TYPE TO BACKUPSET;
CONFIGURE CHANNEL DEVICE TYPE DISK FORMAT '/rmanfs/dbimage/full/%U.dbf';
```

2. Run the RMAN backup with the following commands. The first backup is a level 0 backup and takes some time, depending on the amount of data to be copied.

```
RUN {
  BACKUP INCREMENTAL LEVEL 1 FOR RECOVER OF COPY WITH TAG 'ORADB_INCR' DATABASE;
  RECOVER COPY OF DATABASE WITH TAG 'ORADB_INCR';
}
```

3. After a successful level 0 backup, create a snapshot on the SolidFire storage for all the volumes that are part of the RMAN file system.
4. Configure the RMAN parameter to update the location for a level 1 backup.

```
CONFIGURE CHANNEL DEVICE TYPE DISK FORMAT '/rmanfs/dbimage/incremental/%U.dbf';
```

5. Create a level 1 backup image by running the same commands from step 2. To simplify this step, you can save the commands to a script file to use on the RMAN command line. You can take the subsequent level 1 backups, depending on the backup schedule.
6. Back up the archive logs. The following command backs up all the archive logs currently known in the control file that have not been backed up to disk yet. After the backup of the archive logs is finished, the control file is updated.

```
BACKUP ARCHIVELOG ALL NOT BACKED UP 1 TIMES;
```

7. Schedule the snapshot on the SolidFire storage to run right after step 6 for all the volumes that are part of the RMAN file system.

7.3 Use Cases for RMAN Merge

- Users can switch to the RMAN merge file, recover the database to a desired point in time, and significantly reduce the recovery time.
- Users can also use a disk-based image copy.
- The snapshots that are taken on the RMAN image can be used to create clone copies of the database easily. The clone copy of the database is created using the final merge image, which has all the changes from the last level 1 backup operation.
- The archive logs can also be applied to the clone copy to apply the latest changes from production.

A sample output of the RMAN target file system is provided in the appendix.

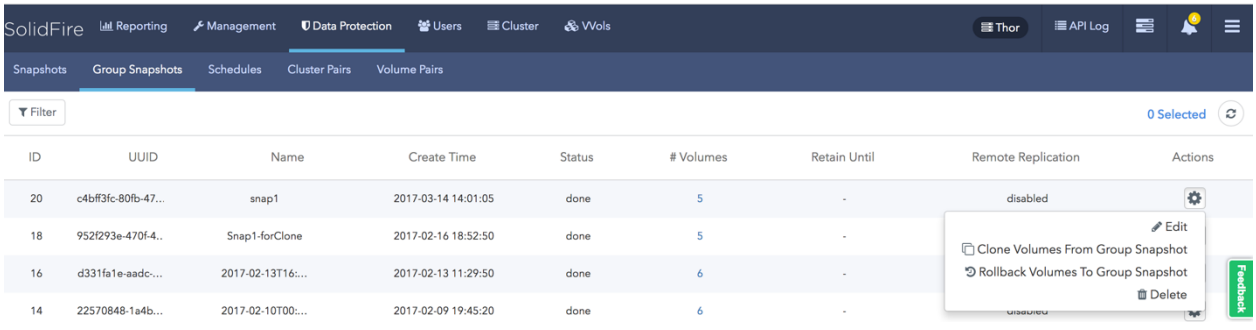
8 Database Cloning

Creating usable, space-efficient, and time-efficient database copies quickly and with virtually no effect on the production system is important. Element volume cloning is a proven technology that helps database and system administrators deliver a near-instantaneous, space-efficient, point-in-time copy of the production database. Traditional methods of copy processing pose various challenges, including system downtime and degraded performance during the cloning process. Also, a large amount of storage space is required to store each clone. The Element volume cloning process is completed quickly, with virtually no performance effect on the production system.

8.1 Clone a Volume

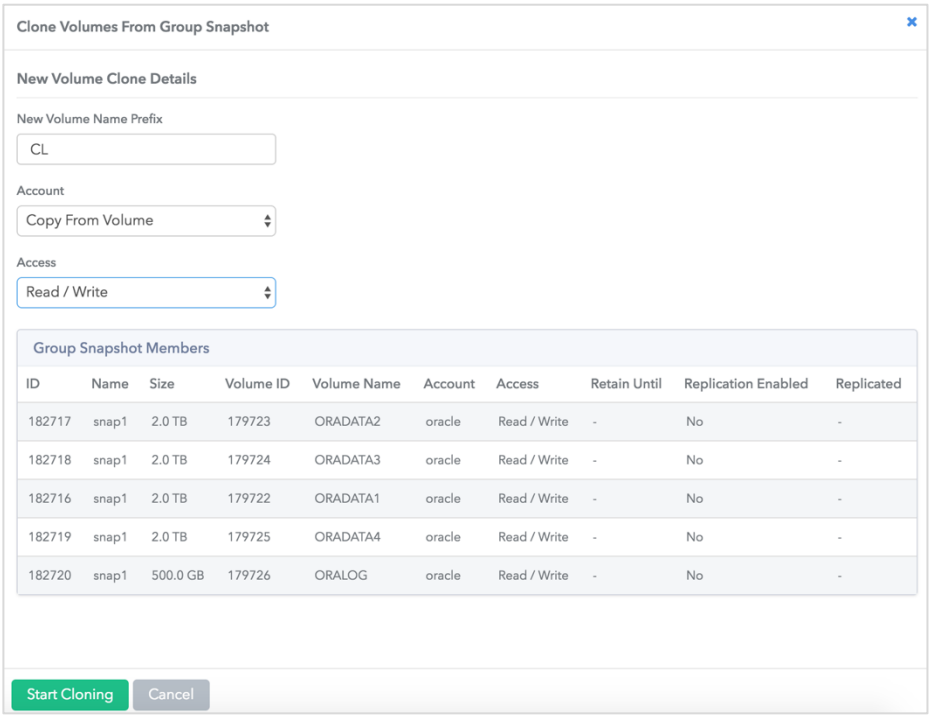
To clone a volume, complete the following steps:

1. Log in to the Element UI.
2. Select Data Protection > Group Snapshots. Right-click the Actions button for the snapshots. In this case, we select Snap1, the snapshot taken in section 8.1.
3. The Clone Volumes from Group Snapshot window opens.

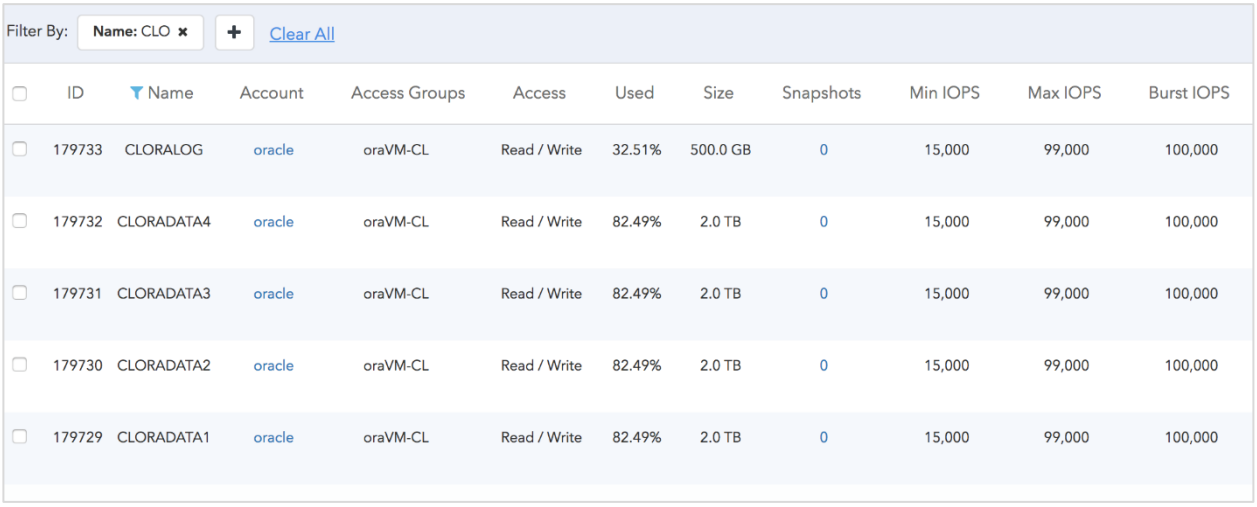


4. Click the gear icon and then select Clone Volumes from Group Snapshot.

5. Enter a prefix (`CL` in this example).
6. Provide the account and access info, depending on what level of access you require for the clone volumes.



7. Click Start Cloning.
8. The cloned volumes can be viewed in the volumes list.



9. After the clone process is complete, add the newly created volumes to the volume access group of the database server (target) where you are planning to host the cloned copy.
10. Log in to the target host.
11. To rescan the iSCSI devices to present the newly cloned volumes, run the following commands:

```
iscsiadm -m discovery -t sendtargets -p <SolidFire SVIP> --op update -n node.session.nr_sessions
-v 2 -> where "n" is the number of paths
```

```
iscsiadm -m node -L all
multipath -r
```

12. Set the permission for the Oracle user or the grid user.
13. Mount the file systems or start the ASM instance.
14. Log in to the Oracle instance.

```
startup mount;
recover database;
alter database open;
```

Appendix A: RMAN Merge Output

```
-rw-r-----. 1 oracle oinstall 6597069774848 Mar 13 09:33 data_D-ORADB_I-2689361952_TS-SLOB_FNO-
5_09ruru1n.dbf
-rw-r-----. 1 oracle oinstall      17080320 Mar 13 09:33 0orv12rp_1_1.dbf
-rw-r-----. 1 oracle oinstall         40960 Mar 13 09:33 0prv12rp_1_1.dbf
-rw-r-----. 1 oracle oinstall       8839168 Mar 13 09:33 0nrv12rp_1_1.dbf
-rw-r-----. 1 oracle oinstall      56811520 Mar 13 09:33 0mrv12rp_1_1.dbf
-rw-r-----. 1 oracle oinstall       1671168 Mar 13 10:14 0trv157p_1_1.dbf
-rw-r-----. 1 oracle oinstall         40960 Mar 13 10:14 0urv157p_1_1.dbf
-rw-r-----. 1 oracle oinstall        286720 Mar 13 10:14 0srv157p_1_1.dbf
-rw-r-----. 1 oracle oinstall       3702784 Mar 13 10:14 0rrv157p_1_1.dbf
-rw-r-----. 1 oracle oinstall       5251072 Mar 13 11:43 data_D-ORADB_I-2689361952_TS-USERS_FNO-
6_0druru1n.dbf
-rw-r-----. 1 oracle oinstall     157294592 Mar 13 11:43 data_D-ORADB_I-2689361952_TS-
UNDOTBS1_FNO-4_0cruru1n.dbf
-rw-r-----. 1 oracle oinstall     838868992 Mar 13 11:43 data_D-ORADB_I-2689361952_TS-SYSTEM_FNO-
1_0bruru1n.dbf
-rw-r-----. 1 oracle oinstall    1027612672 Mar 13 11:43 data_D-ORADB_I-2689361952_TS-SYSAUX_FNO-
3_0aruru1n.dbf
-rw-r-----. 1 oracle oinstall       1900544 Mar 13 11:43 12rv1aep_1_1.dbf
-rw-r-----. 1 oracle oinstall         40960 Mar 13 11:43 13rv1aep_1_1.dbf
-rw-r-----. 1 oracle oinstall        294912 Mar 13 11:43 11rv1aeo_1_1.dbf
-rw-r-----. 1 oracle oinstall       4153344 Mar 13 11:43 10rv1aeo_1_1.dbf
-rw-r-----. 1 oracle oinstall         40960 Mar 13 13:08 01rv12rp_1_1.dbf
-rw-r-----. 1 oracle oinstall         40960 Mar 13 14:02 0qrv157p_1_1.dbf
-rw-r-----. 1 oracle oinstall         40960 Mar 13 15:07 0vrv1aeo_1_1.dbf
```

Where to Find Additional Information

To learn more about the information that is described in this document, review the following documents and websites:

- DS-3881: NetApp HCI Datasheet
  https://www.netapp.com/us/media/ds-3881.pdf
- TR-4644: NetApp SolidFire Quality of Service (QoS)
  https://www.netapp.com/us/media/tr-4644.pdf
- TR-4651: NetApp SolidFire SnapMirror Architecture and Configuration
  https://www.netapp.com/us/media/tr-4651.pdf
- TR-4641: NetApp HCI Data Protection
  https://www.netapp.com/us/media/tr-4641.pdf
- TR-4639: Element Software Linux Configuration Guide
  www.netapp.com/us/media/tr-4639.pdf
- NVA-1122: VMware Private Cloud on NetApp HCI
  www.netapp.com/us/media/nva-1122-design.pdf
  www.netapp.com/us/media/nva-1122-deploy.pdf
- TR-4748: Build Your NetApp Data Fabric
  www.netapp.com/us/media/tr-4748.pdf

- TR-4643: Element Software Windows Configuration Guide
  https://www.netapp.com/us/media/tr-4643.pdf
- NetApp product documentation
  https://docs.netapp.com

Version History

Version	Date		Document Version History
Version 1.0	April 2019		Initial document release.
Version 2.0	July 2020		Merged Oracle on SolidFire (TR-4606) material; reviewed content.

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

Trademark Information

TR-4768-0820