Executive Overview

Oracle Maximum Availability Architecture (MAA) is the Oracle best practices blueprint for implementing Oracle high availability technologies. Maximum Availability Architecture is one of the key requirements for any Oracle Fusion Middleware enterprise deployment. Oracle Fusion Middleware includes an extensive set of high availability features such as: process death detection and restart, server clustering, server migration, clusterware integration, GridLink, load balancing, failover, backup and recovery, rolling upgrades, and rolling configuration changes, which protect an Enterprise Deployment from unplanned downtime and minimize planned downtime needs.

Oracle Exalogic is an integrated hardware and software system designed to provide a complete platform for a wide range of application types and widely varied workloads. Exalogic is intended for large-scale, performance-sensitive, mission-critical application deployments. The Exalogic system contains many redundant components to ensure that the failure of any single component does not affect overall system availability. Whilst this built-in redundancy can cope with hardware component failures it cannot protect against:

- Complete Exalogic system failure.
- Media Failure
- User Error - User updates or deletes something that they did not plan on doing.

To recover from these types of errors the system must be able to be restored to either the same or new hardware. Critical systems will often be protected using disaster recovery (DR) technologies. These usually take the form of a similar system located off site, which is automatically kept up to date with changes made on the primary system as and when they occur. These systems provide hot standby capability in the event of the primary system failure.
Whilst hot standby systems are extremely useful for business continuity, they are expensive to maintain and need additional infrastructure. In some circumstances such as simple user errors, it may be quicker to fix the issue than to failover to the DR system especially when DNS needs updating.

Taking regular backups of a system is part of standard operating procedure for most production systems and is done irrespective of whether or not the site has a Disaster Recovery solution. It allows the flexibility to restore individual files should something happen to the original or the system as whole. Backups can also be stored off site in a secure location. Backups on Exalogic can be within the Exalogic system, disk-to-disk and disk-to-tape and this paper describes the options available when using Exalogic for all these cases. The specific combination that should be used for a particular deployment depends on the requirements of the site.

Exalogic comes with Sun ZFS storage 7320 appliance and this paper describes how to leverage some built in feature of the storage for disk based backups. When backing up to tape you have the option of using NDMP or via backup agents deployed to the compute node. NDMP allows the tape backup software to interact directly with the storage appliance rather than going via the operating system and therefore will be faster, and have no overhead on the compute nodes of Exalogic, however it cannot be used to backup the operating system, or any other files, which are stored on local storage. If speed of backup is an issue then the fastest solution would be to use NDMP, however taking the backup from the compute node is more flexible.

The Backup and Recovery Solutions for the Oracle Exadata Machine and Oracle Exalogic Machine build upon well-established solutions for Oracle Databases and Oracle Fusion Middleware respectively. Whilst the solution described in this white paper for Disk to Tape backups utilizes Oracle Secure Backup the mechanism described can be applied to any tape media management solution.
Introduction

This paper concentrates on backing up (and restoring) data held within the Oracle Exalogic Machine.

The data contained in an Oracle Exalogic Machine which needs to be backed up consists of:

- Exalogic Operating System
- Software Binaries
- Configuration Information
- Transactional Data, such as Transaction Logs as JMS Queues.
- Switch Configuration
- Other Artifacts which are stored on disk.

These objects can be backed up to:

- Disk within the same storage appliance.
- Disk on a remote machine, which utilizes the same storage type (ZFS).
- Disk on a remote machine, which utilizes a different storage type.
- Tape.
A backup strategy is likely to encompass more than one of the above. This white paper covers the best ways of achieving these backups, and restoring from them.
Concepts

Backup and Recovery Concepts

Volatility

Objects can be grouped by volatility; for example, the operating system changes very infrequently and therefore does not need backing up as frequently as transactional data, which changes on a frequent basis. In a typical Exalogic deployment objects can be grouped into the following categories:

<table>
<thead>
<tr>
<th>VOLATILITY GROUP</th>
<th>EXAMPLE OBJECTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>Oracle Binaries</td>
</tr>
<tr>
<td></td>
<td>Operating System</td>
</tr>
<tr>
<td>Medium</td>
<td>Configuration Information</td>
</tr>
<tr>
<td></td>
<td>- WLS Domain</td>
</tr>
<tr>
<td></td>
<td>- Oracle Instance</td>
</tr>
<tr>
<td>High</td>
<td>File based JMS Queues</td>
</tr>
<tr>
<td></td>
<td>Persistent Stores</td>
</tr>
</tbody>
</table>

Backup Frequency

The volatility of the data can be used to determine backup frequency. In addition to volatility the following may impact the frequency in which data is backed up:

- Volume of data to be backed up.
- Available backup windows.
- Regulatory requirements.

Using the above volatility groups, the following would be a sensible backup frequency:

<table>
<thead>
<tr>
<th>VOLATILITY GROUP</th>
<th>BACKUP FREQUENCY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>Monthly</td>
</tr>
<tr>
<td>Medium</td>
<td>Weekly</td>
</tr>
</tbody>
</table>
In addition to the scheduled backups, it makes sense to perform ad-hoc backups when major events occur. For example, it is appropriate to take an additional backup of the Oracle binaries after patching or upgrade.

**Retention Periods**

In determining a backup strategy, you need to factor in how long you wish to keep the backups for. This is mainly dependent on your business and regulatory requirements; using the examples above the following may be appropriate values.

<table>
<thead>
<tr>
<th>VOLATILITY GROUP</th>
<th>RETENTION PERIOD</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>3 years</td>
</tr>
<tr>
<td>Medium</td>
<td>6 months</td>
</tr>
<tr>
<td>High</td>
<td>7 days</td>
</tr>
</tbody>
</table>

**Backup Types**

There are two different types of backups available, full backups and incremental backups. A full backup backs up the entire file system as it is at that moment in time. An incremental backup backs up only the data that has changed since the last backup. Incremental backups can be either cumulative or differential. A cumulative backup backs up all the changes since the last full backup, whilst a differential backup backs up the changes since the last differential – differential backups are not supported on ZFS storage appliances, they are however widely available when backing up to tape.

Incremental backups can be leveled. That is you can perform a level 0 (full backup) each month, a level 1 (incremental) each Sunday and a level 2 (incremental) each weekday. If this type of strategy is implemented then only the data that has changed since the last level -1 backup is backed up. For example on Tuesday, the data backed up is the data, which has changed since the last level 1 backup that was taken on the previous Sunday. Incremental backups are useful when the volume of data to be backed up is significant.

The advantage of a full backup is that the backup contains all of the information required to perform a restore. In an incremental backup strategy, a restore is likely to use several backups. In the 3 level backup strategy above you would need, the Last level 0 backup, plus the last level 1 backup taken, plus the last level 2 backup taken. If the volume of data to be backed up is small, then it may be easier to perform a full backup each time rather than an incremental one, but this will be determined by the volumes of data being backed up.

Incremental backups are supported by Oracle Secure Backup and the operating system dump command.
Note: The typical usage of an incremental backup strategy is to perform a complete backup once a week and an incremental cumulative once a day, however as data volumes increase a multi-leveled approach may be more suitable.

A backup can be taken Hot (when processes are running) or Cold when processes are shutdown. The advantage of a cold backup is that when taken everything is in a consistent state. The disadvantage of a cold backup is that whilst the backup is being undertaken systems are not available. Some of the methods described below allow a consistent backup to be taken without the need for downtime. Whether or not a hot backup is possible will depend on the artifacts being backed up. You should contact your software vendor to see whether the product you wish to back up can be backed up whilst running. Oracle Fusion Middleware supports hot backups.

Exalogic Backup Technologies

Snapshots

ZFS uses a copy-on-write transactional model. This means that when ZFS writes new data, the blocks containing the old data are retained. A snapshot is an internal copy of what data blocks are current at a moment in time. Taking a snapshot is fast because it only stores the block locations it does not need to backup the data blocks directly as they already exist. As such snapshots consume little space.

Benefits:

- Fast backup and restore.
- Provides a consistent backup at a given point in time.
- Snapshots can be made available on disk to allow the restoration of individual files.
- Can be used as part of a DR strategy.
- Can be backed up to tape.
- Once replicated, to a remote ZFS appliance, the snapshot can be mounted on a host which has access to the remote server, and then backed up to tape from there ensuring that there is very little overhead on the source machines.

Drawbacks:

- Restoring a Snapshot restores the entire snapshot data set.
- Cannot be used to backup local file systems for example the operating systems.
- Does not protect against complete storage appliance failure.

Operating System Utilities

These are the traditional methods of making a backup. It involves manually creating a backup file using a operating system commands such as tar, dump or rsync.
Benefits:

- Can be restored on any system.
- Individual files can be restored.

Drawbacks:

- Can be slow to produce. It is dependent on the shares involved.
- Does not guarantee consistent backup at a point in time, although this can be mitigated by backing up from a snapshot.

Remote Disk Backups to a ZFS Storage Appliance

Backups can be made to remote disks. If the remote disk is another ZFS storage appliance then this can be achieved using snapshot replication.

Benefits

- Protects against total loss storage appliance.
- Can be incorporated into a DR strategy.
- Uses built in functionality of the storage appliance

Drawbacks

- Cannot be used to backup local disks.

Remote Disk Backups to a non ZFS Storage Appliance

Backups can be made to remote disks. If the remote disk is not another ZFS storage appliance then this can be achieved using operating system utilities, which write to a network mount.

Benefits

- Protects against total loss storage appliance.
- Can be used to backup local disks.

Drawbacks

- Cannot use built in functionality of the storage appliance
- Can be slow to produce depending on network and backup volume.

Tape Media Manager

If archiving to tape a tape media manager is required. The media manager catalogues and manages the physical tape media, as well as acting as the interface between the Exalogic machine and the tape
library. A Media manager can backup to physical or virtual tape libraries. Oracle recommends using Oracle Secure Backup for this purpose, although others can be used if desired. Backing up to tape can be used in conjunction with other backup methods to provide a tiered approach.

Benefits

- Can keep many different backup versions for indefinite periods.
- Backups can be duplicated and held at more than one off site location.
- Physical tapes are managed by the media manager.
- Backups can be made to a physical tape library or to disk using a virtual tape library.

Drawbacks

- Backup can be slower depending on the environment.
- Restore can be slower if the backup to be restored is not on-site/in the tape library.

Backup Strategy

There are many methods of putting together a backup strategy and these are largely dependent on the backup devices in play. A possible backup strategy however would be:

1. Create local Snapshots, for fast restores and recoveries from user error.
2. Create tape backups for archive storage in case of machine failure.

For complete recovery sets, the snapshot can be backed up directly to tape. If near line disk backups are required, disk-to-disk backup using remote replication to ZFS storage is recommended and backups to tape can be done off the remote storage.

Note: When backing up the Exalogic machine, coordinate the backup schedule with that of any attached databases to ensure a consistent restore.

Oracle Secure Backup Concepts

Oracle Secure Backup, is Oracle’s enterprise tape management system. It allows backups to be made to tape devices; these backups can be encrypted for added security. Oracle Secure backup, not only facilitates backups to tape, but it also:

- Keeps track of what has been backed up where.
- Keeps track of when media can be reused.
- Allows tape vaulting.
Oracle Secure Backup is used in this document to illustrate how the Exalogic Machine can be backed up to tape. Oracle Secure Backup consists of a number of components, which are explained below.

**Administrative Domain**

An Oracle Secure Backup administrative domain is the sum of the Administrative server plus media servers plus tape libraries plus all of the hosts, which are backed up.

**Administration Server**

The administration server is the host that stores configuration information for the administrative domain. It contains the backup catalogue and a job scheduler, which is responsible for initiating backups, and restores.

**Media Server(s)**

Media servers are computers or servers to which a tape drive or silo is attached. A media server is responsible for transferring data to or from the tape devices that are either directly attached or Storage Area Network (SAN) attached.

**Client**

A client is any computer or storage device whose files Oracle Secure Backup backs up or restores.

It is the client that is used to perform the backup. In an Exalogic Machine you install the OSB software on the Exalogic compute nodes to be backed up.

It is possible for OSB to interact with the storage appliance directly without the need to install the OSB client software. This is achieved by using the Network Data Management Protocol (NDMP). If the NDMP protocol is used then there is the additional option of backing up a ZFS storage appliance using either the NDMP backup type zfs or dump options.

If NDMP dump is used then files are backed up on a file-by-file basis and can be restored as such, to ensure a read consistent view of the data, NDMP dump first initiates a snapshot.

If NDMP zfs backup type is used this will backup the entire project/filesystem in one go. It does so by first creating a snapshot that it then disposes of it after the backup is complete. The downside to this approach is that it is not possible to restore individual files, it is however very performant. To get round this the backup could be restored to a different location and individual files extracted from there.

**Media Family**

A media family is tape pool is a logical classification of tapes, which have common attributes. Media families are used to group backups with similar retention, duplication and vaulting requirements on to the same tapes.
For example if you wish to keep your high volatility backups for 7 days and your low volatility backups for 1 year, then you would have two different media families one with a retention period of 7 days and one with a retention period of 1 year.

**Backup Catalogue**

The Oracle Secure Backup catalogue is stored on the administrations server. The catalogue stores all information pertaining to the backup domain such as:

- Configuration data regarding hosts, devices, users etc.
- Backup metadata.
- User defined backup schedules.
- Tapes – Associated backups, duplicates, retention periods and location.

As can be seen from the list above the information contained within the backup catalogue is crucial for backing and restoring Exalogic Machines within the administrative domain. This catalogue must be backed up as well. For information on how to do this see the [Oracle Secure Backup Administration Guide](#).

**Configuring Oracle Secure Backup**

Configuring Oracle Secure backup is outside of the scope of this document, for details on how to configure Oracle Secure Backup, refer to the [Oracle Secure Backup documentation](#).

**Connecting External Devices to the Exalogic Machine**

This section of the paper describes how to connect and configure your Exalogic Machine to external devices for the purposes of performing a remote backup. You would connect an external device if you wish to perform one of the following backup types:

- Backup to a remote ZFS storage device
- Backup to a remote storage appliance, which does not utilize ZFS.
- Backup to a remote tape.

**Connecting to a Remote Storage Appliance**

How you connect, the remote storage appliance depends on the type of network the remote storage appliance supports. If it is another ZFS storage appliance this can be connected using infiniband, if however the remote storage appliance does not support infiniband, it should be connected using the fastest Ethernet connection available.
Figure 1 – Exalogic to ZFS

Figure 2 – Exalogic to non-ZFS storage

- Figure 1 describes a remote disk backup solution with a ZFS storage appliance attached directly to the Exalogic Machine using the existing infiniband framework.
- Figure 2 describes a remote disk backup solution with a storage appliance attached directly to the Exalogic Machine using Ethernet.
Note: It is not mandatory to connect remote ZFS appliances using infiniband.

If connecting the storage appliance via infiniband each storage appliance requires an InfiniBand QDR HCA or the recommended dual-ported InfiniBand QDR HCA which is compliant with the Exalogic infiniband network. The network protocol used for backups over InfiniBand is the IpoIB which uses the hosts TCP/IP framework, so it is transparent to the backup software.

The backup software operates identically whether using InfiniBand or a Gigabit Ethernet network.

InfiniBand connections must use the Leaf switches rather than the spine switches.

Connecting to a Tape Management Device

Figure 3 – Exalogic to StorageTek
Figure 4 – Exalogic and Exadata to StorageTek
Figure 5 - Exalogic and Exadata shared Infrastructure
• Figure 3 describes a tape backup solution with two or more media servers attached directly to the Exalogic Machine.

• Figure 4 shows an Exalogic/Exadata hybrid topology with each machine having its own set of Oracle Secure Backup media servers.

• Figure 5 shows an Exalogic/Exadata hybrid topology with each machine sharing the same set of media servers.

In each case the media servers are connected to the existing InfiniBand fabric using the spare HA-bonded ports available on the Exalogic/Exadata Machines. Which solution you choose will depend on the volume of data you wish to backup. If there is only a small amount of data in addition to the data on the Exadata machine, then option 3 would be the most appropriate.

Each media server requires an InfiniBand QDR HCA. The network protocol used for backups over InfiniBand is the IPoIB protocol, so it is transparent to the backup software on the database servers and the media servers. The backup software operates identically whether using InfiniBand or a Gigabit Ethernet network.

The media servers must be connected to the Leaf switches rather than the spine switches.

Whilst it is possible to connect Exalogic systems to existing Exadata systems that have media servers directly attached to the InfiniBand leaf switches this is not recommended as this media server cannot be securely isolated from Exalogic InfiniBand fabric. The recommended alternative is to connect such media servers via Ethernet.

When Oracle Secure Backup (OSB) is used, it is recommended that OSB be installed on a validated hardware configuration such as

• X2270 M2, X4170 M2, X4270 M2 or X4470 M2 servers

• Sun InfiniBand QDR Host Channel Adapter: Low Profile, with the same driver version used by the Exalogic system

• Oracle Linux UEK 64-bit version 5 update 5 (or later) or Solaris 11”

If you are combining your Exalogic Machine with an Oracle Exadata Machine for the databases, then the two machines can share the same backup infrastructure.

Creating a Backup Network

If you are backing up to a remote device be it disk or tape, you should create a dedicated backup network, creating a backup network will allow you to separate backup traffic from user traffic to avoid the two competing with each other.

When performing remote disk backups to a remote storage appliance, it is recommended to create a dedicated backup network, to prevent contention on the client network. If you are backing up to a remote ZFS storage server then this is achieved by creating a storage replication channel.

If you are backing up to a remote non zfs storage appliance then you should create a dedicated Ethernet network between the Exalogic machine and the remote storage server. This also applies if
connecting your Oracle Secure backup Media Server to your Exalogic machine using Ethernet rather than Infiniband.

Creating a Storage Replication Channel

A storage replication channel is a network channel that is dedicated specifically to replication traffic between the Sun ZFS Storage 7320 appliance at the production site and the backup site. The storage replication channel must be configured on both the production site and standby site before configuring remote replication. This section provides the steps to configure the storage replication channel.

Prerequisites

1. Connect the port igb2 from both the storage heads in the Exalogic Machine to the embedded Cisco Catalyst 4948 switch within the Exalogic Machine.
2. Connect port igb3 from both the storage heads in the Exalogic Machine to a network drop in your data center. This can be a distribution switch in your datacenter.
3. Ensure that the IP address assigned to the replication channel has been provisioned and is in DNS.
4. Oracle recommends provisioning the replication channel IP address on a subnet that is different from the Management IP subnet.

Create Storage Replication Channel

Follow the steps below to configure the storage replication channel. All these steps must be completed on both the production site and the standby site.

1. Open the Browser User Interface (BUI) for the storage head.
2. Navigate to Configuration - Network to bring up the Network screen.
3. Validate that the Built-in Devices igb2 and igb3 are connected and live.
4. Create Datalinks for these two devices.
5. Create the first datalink as follows: Click + Next to Datalinks table to bring up the Network Datalink screen. Enter the following details:
   - Name: Enter a name for the datalink. For example: repl-1-dl
   - Under Devices, choose igb2
   - Accept the default values for all other fields
   - Click Apply to apply the changes.
6. Create the second datalink as follows: Click + Next to Datalinks table to bring up the Network Datalink screen. Enter the following details:
   - Name: Enter a name for the datalink. For example: repl-2-dl
   - Under Devices, select igb3
Accept the default values for all other fields
Click Apply to apply the changes

7. Next create the interfaces for the two datalinks created in steps 5 and 6.

8. Create the first interface as follows: Click + Next to Interfaces table to bring up the Network Interfaces screen.
Enter the following details:
- Name: Enter a name for the interface. For example: repl-1-interface
- Under Properties, unselect Allow Administration
- Select Use IPv4 Protocol.
- Under the Use IPv4 Protocol Section:
  - Choose Static Address List
  - Enter IP Address: 0.0.0.0/8
- Under the Datalinks section select repl-1-dl
- Accept the default values for all other fields
- Click Apply to apply the changes

9. Create the second interface as follows: Click + Next to Interfaces table to bring up the Network Interfaces screen.
Enter the following details:
- Name: Enter a name for the interface. For example: repl-2-interface
- Under Properties, unselect Allow Administration
- Select Use IPv4 Protocol.
- Under the Use IPv4 Protocol Section:
  - Choose Static Address List
  - Enter IP Address: 0.0.0.0/8
- Under the Datalinks section select repl-2-dl
- Accept the default values for all other fields
- Click Apply to apply the changes

10. Create an Active/Passive bonded interface between the interfaces created in steps 8 and 9. This is accomplished by configuring an IPMP group (IP MultiPathing).

11. Create the IPMP group as follows. Click + next to the Interfaces table to bring up the Network Interfaces screen.
Enter the following details:

Name: Enter a name for the interface. For example: \texttt{bak-repl-interface}

Deselect Allow Administration

Select \textbf{Use IPv4 Protocol}.

Under the Use IPv4 Protocol section:

- Choose Static Address List
- Enter the IP address provisioned for the storage replication channel on the production site. Use the format: IPv4Address/mask. For example: \texttt{10.204.77.120/24}, where 10.204.77.120 is the IP address and the 24 is the subnet netmask.
- Use the IP address provisioned for the storage replication channel on the standby site when executing this step on the standby site.

Select \textbf{IP MultiPathing Group}

From the list of interfaces select the interfaces created in steps 9 and 10. For example: select \texttt{repl-1-interface} and \texttt{repl-2-interface}

Set one of the interfaces to \textbf{Active} and the other to \textbf{Standby}.

Click Apply to apply the changes

12. Click Apply on the Network page to apply the configuration changes.

13. Create a routing table entry for the replication interface.

Navigate to the Configuration – Network - Routing

Create a Routing Table Entry as follows: Click + Next to Routing Table Entry table to bring up the Insert Route screen.

Enter the following details:

- Family: Select IPv4
- Kind: \textbf{Default}
- Gateway: The Gateway IP address for the Replication Channel IP address. Use the appropriate Gateway IP address for the production site and standby site
- Interface: Select the IPMP group created in step 11. For example: \texttt{bak-repl-interface}.
- Click Add to add the entry

12. Validate the configuration, by pinging the replication channel IP address from one of

\textbf{Configuring the Gigabit Ethernet (GigE or 10GigE) Network to Remote NFS Server/Media Server}
When connecting the media servers to Exalogic Machine through Ethernet, or connecting the Exalogic storage appliance to a remote disk (non zfs) via Ethernet, connect using one of the GigE interfaces on the storage appliance into the data center network. For high availability, multiple network interfaces on the Exalogic storage servers and multiple network interfaces on the remote nfs disk/media server can be bonded together. In this configuration, configure the interfaces in an active/passive way.

If throughput is a concern, connect both the GigE interfaces from each Exalogic storage server directly into the data center’s redundant network. The two interfaces can then be bonded together in a redundant and aggregated way to provide increased throughput and redundancy. Follow these best practices:

- **Configure the Gigabit or 10 Gigabit Ethernet switch configuration.**
  
  For optimal throughput and availability, configure hardware Link Aggregation in the gigabit switch. The Link Aggregation Control Protocol (LACP)8 is defined as part of IEEE 802.1AX-2008 standard. Other software enabled bonding options are available within the operating system of the storage servers and media server, which may also be used.

  If you are using LACP, then ensure that LACP is supported and configured on the Ethernet switch for Src XOR Dst TCP/UDP Port. See your vendor’s Gigabit switch documentation for information about configuring source and destination port load balancing.

- **Configure the media server Gigabit or 10Gigabit Ethernet.**
  
  The following recommendations are applicable only for media servers running Oracle Enterprise Linux Version 5.3 (or later) or RedHat Enterprise Linux Version 5.3 (or later). If your specific media server is running a different operating system, contact your vendor for the appropriate Gigabit configuration.

  As with the storage server Gigabit Ethernet configuration, no specific changes must be made to the media servers. However, to obtain higher backup rates, create a Multiple-Ported Gigabit or 10Gigabit Ethernet Configuration. The steps to configure bonding on the media server are the same as on the database servers. See the Oracle Exadata Storage Server Software User's Guide for a detailed procedure.

**Configuring InfiniBand Network**

With the available InfiniBand ports in a Exalogic Machine, media servers or remote storage appliances supporting InfiniBand can be directly connected to the infiniband fabric by adding an InfiniBand Quad Data Rate (QDR) host channel adapter (QDR HCA) to the media server. For high availability, connect the HCA to two different Exalogic Machine InfiniBand leaf switches to eliminate the switch as a single point of failure. This provides seamless failover if connectivity is lost to one of the ports.

Follow these best practices.

Note: The examples included with each bullet are based on a media serve running on the Linux operating system. For storage appliances supporting InfiniBand you should consult your vendor documentation.
- Configure bonding of the InfiniBand interfaces on the media server.
  The following example of bonding ib0 and ib1 is specific to a Linux environment:

1. Modify the `/etc/modprobe.conf` file to add the following two lines to the bottom of the file. This adds another bonding alias and options.
   alias bondib0 bonding
   options bonding max_bonds=10

   Note: Depending on how many bonded network interfaces are required in the media server, you may need to adjust this value accordingly. In this example, a value of 10 is assumed.

   The file will be similar to the following example. This file assumes bonding was previously established on bond0:

   alias ib0 ib_ipoib
   alias ib1 ib_ipoib
   alias bondeth0 bonding
   alias bondib0 bonding
   options bonding max_bonds=2

2. Create the `/etc/sysconfig/network-scripts/ifcfg-bondib0` file, as follows.
   DEVICE=bondib0
   USERCTL=no
   BOOTPROTO=none
   ONBOOT=yes
   IPADDR=<IP Address for bondib0 within the same subnet as the existing InfiniBand network >
   NETMASK=<Netmask must be the same as the existing InfiniBand network >
   NETWORK=<Network calculated using ipcalc-n ip_address netmask>
   BONDING_OPTS="mode=active-backup miimon=100 downdelay=5000 updelay=5000"
   IPV6INIT=no

3. Make copies of the current ib0 and ib1 configuration files. Ensure the copied files do not start with ifcfg-ib0. Prefix the file name with backup- or a similar word, and do not add a suffix such as -backup. For example:
cd /etc/sysconfig/network-scripts/
cp ifcfg-ib0 backup-ifcfg-ib0
cp ifcfg-ib1 backup-ifcfg-ib1

4. Modify the current ib0 and ib1 configuration files so they are configured to act as slaves to the bondib0 interface. The files should appear as follows:
   * File ifcfg-ib0:
     DEVICE=ib0
     USERCTL=no
     ONBOOT=yes
     MASTER=bondib0
     SLAVE=yes
     HOTPLUG=no
     BOOTPROTO=none
     MTU=65520

   * File ifcfg-ib1:
     DEVICE=ib1
     USERCTL=no
     ONBOOT=yes
     MASTER=bondib0
     SLAVE=yes
     HOTPLUG=no
     BOOTPROTO=none
     MTU=65520

5. Restart the system, network interface or service as appropriate.

6. Log in as the root user after the system restarts to verify that NIC bonding is running correctly.
   # cat /proc/net/bonding/bondib0

   Ethernet Channel Bonding Driver: v3.5.0 (November 4, 2008)
Bonding Mode: load balancing (round-robin)
MII Status: down
MII Polling Interval (ms): 0
Up Delay (ms): 0
Down Delay (ms): 0

[root@adce01cn03 ~]# cat /proc/net/bonding/bond0
    Ethernet Channel Bonding Driver: v3.5.0 (November 4, 2008)

    Bonding Mode: fault-tolerance (active-backup) (fail_over_mac active)
    Primary Slave: None
    Currently Active Slave: ib1
    MII Status: up
    MII Polling Interval (ms): 100
    Up Delay (ms): 5000
    Down Delay (ms): 5000

    Slave Interface: ib0
    MII Status: up
    Link Failure Count: 2
    Permanent HW addr: 80:00:00:4a:fe:80

    Slave Interface: ib1
    MII Status: up
    Link Failure Count: 0
    Permanent HW addr: 80:00:00:4b:fe:80

• Update OpenFabrics Enterprise Distribution on the media server.
  You must use an OpenFabrics Enterprise Distribution (OFED) version that is compatible
  with the version found in Exalogic Machine in the media server. You can download the
  OFED from My Oracle Support Note 888828.1.
• Configure InfiniBand IPoIB connected mode for best performance.
No changes are required to the compute nodes of Exalogic Machine running Exalogic 11g Release 2 (11.2.0.2) and later. However, for custom configurations, you must evaluate the following settings.

The following commands assume a Linux operating system.

1. Verify that Connected Mode is enabled on the system, as follows:
   
   ```
   # cat /sys/class/net/ib0/mode
   connected
   
   # cat /sys/class/net/ib1/mode
   connected
   ```

   If the status is “Datagram,” then proceed to step 2 and step 3.

2. Edit the `/etc/ofed/openib.conf` file and search for `SET_IPOIB_CM` and change its value to specify “yes”:

   ```
   # Enable IPoIB Connected Mode
   SET_IPOIB_CM=yes
   IPOIB_LOAD=yes
   ```

3. Reboot the server and re-verify the connected mode again, following the instructions in step 1.

   - Configure MTU Size=65520 on InfiniBand for faster data transmission.

No changes are required to the compute nodes of an Exalogic Machine running Exalogic 11g Release 2 (11.2.0.2) and later releases. However, for custom configurations, you must evaluate the following settings:

1. Edit the `/etc/sysconfig/network-scripts/ifcfg-ib*` and the `/etc/sysconfig/network-scripts/ifcfg-bondib0` files to add an entry for MTU=65520. For example:

   ```
   MTU=65520
   ```

2. Verify that the MTU size is 65520, as follows:

   ```
   # ifconfig ib0 | grep MTU
   UP BROADCAST RUNNING SLAVE MULTICAST MTU:65520 Metric:1
   
   # ifconfig ib1 | grep MTU
   UP BROADCAST RUNNING SLAVE MULTICAST MTU:65520 Metric:1
   
   # ifconfig bondib0 | grep MTU
   UP BROADCAST RUNNING MASTER MULTICAST MTU:65520 Metric:1
   ```
3. Reboot the server and verify the MTU size again, following the instructions in step 1.

- Configure the media server to use the InfiniBand network.

To direct the backup and restore traffic over the InfiniBand fabric, configure the media management software to favor InfiniBand. Note that each media management software type has its own method of enabling this configuration.

For instance, Oracle Secure Backup has the concept of a preferred network interface, which can be set on the media server for a specific list of clients. Other media management software requires this configuration to be defined when the software is installed. See your media management software for information about how to direct traffic over a particular network.

Configuring Persistent Bindings for Tape Devices

In SAN environments, you must configure persistent bindings so the device address does not change. If the device address changes, the media servers cannot access the device unless you update the device configuration within Oracle Secure Backup. Therefore, it is very important that your environment maintains consistent device addresses.

Persistent bindings are not configured within Oracle Secure Backup but they are a part of your infrastructure setup. You may configure persistent bindings through the HBA or the operating system. The configuration steps may vary by platform and vendor. See My Oracle Support Note: 971386.1 for an example of creating persistent bindings for device attachments.

Connecting External Devices using a VLAN

If you are connecting your remote backup device using an existing datacenter network, you may need to use Virtual LANs (VLANs to connect to existing systems in datacenter networks. Exalogic System supports 802.1Q standard VLAN implementations in the network. Following sections provide necessary information on how to do such configurations on different components inside Exalogic. Detailed information can also be obtained through their respective documentations.

Creating VLAN based network interfaces from Exalogic compute nodes

Exalogic compute nodes have two type of network interfaces.

a) Four 1Gbps Ethernet ports
b) Two InfiniBand ports

Depending on overall network design and architecture, we can use either of these to connect to external systems for backup and recovery using VLANs. This section is sub divided into two parts for easier understanding.

Manual VLAN configuration on standalone 1GbE network interfaces
At least one of the four 1Gbps Ethernet port is pre-wired to internal Cisco switch for management network. Any remaining port can be used for a direct access to the compute node over a Gigabit network. Under Linux, a VLAN tagged interface can be created as follows.

1. Load the necessary kernel module
   
   ```bash
   # modprobe 8021q
   ```

2. Verify this module is now loaded
   
   ```bash
   # lsmod | grep 8021q
   ```

3. Add a VLAN tag to an interface e.g. VLAN 25 to eth3
   
   ```bash
   # vconfig add eth3 25
   ```

4. Verify that VLAN has been added to interface
   
   ```bash
   # cat /proc/net/vlan/config
   ```

Assign an IP address to VLAN tagged interface. Such interfaces appear in Linux as

```bash
[Interface_Name]:[Vlan_Tag]
```

```bash
# ifconfig eth3.25 <ip address> <subnet mask> up
```

To make such configurations persistent across reboots, you need to create scripts like any other interface in Linux.

```bash
/etc/sysconfig/network-scripts/ifcfg-eth3.25
```

Make sure to update two specific parameters for VLAN based interface scripts as follows:

```bash
DEVICE=eth3.25  # This means the device is eth3 with VLAN ID 25
VLAN=yes
```

**VLAN configuration over Linux Bonded Interfaces**

In order to achieve high availability, we can use a pair of bonded physical interfaces under VLAN. Its recommended to first create the bonded interface based on two or more physical interfaces and then assign a VLAN tag on the bonded interface. For example, if bond3 has been created from eth2 and eth3, then assign VLAN tag to bond3. This is illustrated below.

First, select two interfaces – eth2 & eth3 and prepare them with active standby linux bonding configuration. Create ifcfg-eth2 and ifcfg-eth3 under /etc/sysconfig/network-scripts/ with following contents:
DEVICE=<device name>  # Use eth2 and eth3 respectively in each ifcfg- file
BOOTPROTO=none
HWADDR=<device’ mac address>  # Use corresponding MAC address here
TYPE=Ethernet
ONBOOT=yes
# Settings for Bond
MASTER=bond3
SLAVE=yes

Create ifcfg-bond3.25 under /etc/sysconfig/network-scripts/ with following contents:

DEVICE=bond3.25
IPADDR=<IP address>
NETMASK=<Subnet Mask>
GATEWAY=<Gateway>
USERCTL=no
BOOTPROTO=none
ONBOOT=yes
VLAN=yes
Bring up the two physical interfaces and associated bond3.25 interface with the following command:

```
# ifup bond3.25
```

You can verify the status of VLAN tagged bonded interface as follows:

```
# ifconfig eth2
# ifconfig eth3
# ifconfig bond3.25
# cat /proc/net/vlan/config
# cat /proc/net/bonding/bond3
```

**Using Infiniband Networks for Backup and Recovery**

Now let's discuss the Infiniband ports and their usage in backup and recovery across datacenter networks. Infiniband provides two types of network interfaces that can be used in OSI layered model.

a) IP over Infiniband (IPoIB)

b) Ethernet over Infiniband (EoIB)

We do not recommend to use IPoIB networks for backup and recovery as these are limited to local LANs only. However, EoIB makes perfect sense to use for backup and recovery activities.

EoIB network interfaces need to be created on NM2GW switch first. Please refer to Exalogic or NM2GW user guides for details. In summary, the following command on NM2GW will create EoIB interfaces. These are also called as Virtual NICs or VNICS.

```
# createvnic <GW ETH port> -guid <Host_port_guid> -mac <assigned_mac> [-vlan <vlan_tag> -pkey <partition_key>]
```

Here you can see that VLAN tag can be assigned while creating VNIC. Once we do that an interface instantiates in the compute node's Linux environment. It can be assigned an IP address now.

Check available VNICS on a host

```
# mlx4_vnic_info -l
```

Assign IP address

```
# ifconfig <vnic> <IP_address> <subnet_mask> up
```

Startup scripts must be created to re-configure such VNICS across reboots. It is very important to include MAC address of the VNIC in their respective ifcfg startup scripts. Please refer to Exalogic user guide for details.
Creating VLAN based network interfaces from Exalogic ZFS Storage Appliance

The storage machine (ZFSSA) inside Exalogic has two interfaces available for any external connectivity purposes. VLAN tags can be implemented either through the Browser user interface or via command line configuration. Detailed information can be obtained through Oracle ZFS 7320 user guide.

Configuring VLAN tagged network interfaces from browser user interface

1. Launch your browser and access the BUI.
2. Navigate to Configuration -> Network
3. Verify that the network devices you plan to use have active links. Observe first column under the title “Devices”.
4. Click on + near Datalinks and you will get a smaller popup window to configure an interface.
5. Fill in a name for the device you plane to use. We recommend using same name as device name. e.g. igb2. Leave all the checkboxes unchecked. Select the device from list and click on “Apply”.
6. Repeat the above step again to create another datalink if you plan to use a pair for High Availability. For example, select igb3.

Now, we can add VLAN tag to the datalinks that we just created.

7. Click on + near Datalinks again to get same popup window to configure.
8. Check on “VLAN” option.
9. Assign a name to the VLAN tagged datalink. For example, igb2-25 and igb3-25
10. Enter the VLAN ID to be used in the VLAN text box.
11. Select the interface datalink from list below and click “Apply”
12. Click “Apply” in the main window to commit Datalink changes.
13. Click+ near Interfaces in the main browser window to add IP address and IPMP configurations
14. Assign a name to the interface. For example, igb2-25-A and igb3-25-B
15. Under IPv4 section, assign an IP address 0.0.0.0/8
16. Select the datalink that was previously created. For example, igb2-25 and igb3-25
17. Make sure both checkboxes are enabled under Properties section to enable and allow administration
18. Click “Apply” to save
19. Repeat steps to create another interface if you are configuring High Availability.
20. Click on + near Interfaces again to create an IPMP based interface.
21. Assign a name. For example, ighb2-3-25-ipmp
22. Enter an IP address that you plan to use for this network. For example, 10.23.12.54/22
23. Check “IP Multipathing Group”
24. Select the two interfaces that were created in previous steps and click on “Apply”
25. Select “Standby” for one of the interface to create an active standby configuration
26. Now, click on the “Apply” on main page to confirm all changes made

Exalogic Disk Configuration

For the purposes of this paper the Exalogic Machine has been setup as per the Exalogic Enterprise Deployment Guide with the following exceptions.

Disk Layout

Projects

In order to create storage areas to reflect the above volatility groups the following projects need to be defined in addition to those described in the Exalogic Enterprise Deployment Guide.

Details of how to create these projects can be found in the Exalogic Enterprise Deployment Guide.

As an example, if you were creating a Fusion Middleware Deployment based on one of the Oracle Fusion Middleware Enterprise deployment guides you may need to create the following:

![Diagram showing network and project configurations]

To achieve this you would create the following projects:
### PROJECT NAME: MW BINARIES

<table>
<thead>
<tr>
<th>PROPERTY NAME</th>
<th>VALUE</th>
<th>COMMENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quota</td>
<td>100GB</td>
<td>Quota for the Project including snapshots. The quota should be allocated based on your requirements.</td>
</tr>
<tr>
<td>Mount Point</td>
<td>export/product/</td>
<td></td>
</tr>
<tr>
<td>All other settings</td>
<td>Default</td>
<td></td>
</tr>
<tr>
<td>Share Name</td>
<td>mw_home1</td>
<td>Share mount point: /export/product/fmw Mounted on apphost1 as /u01/app/oracle/product</td>
</tr>
<tr>
<td>Share Name</td>
<td>mw_home2</td>
<td>Share mount point: /export/product/fmw Mounted on apphost2 as /u01/app/oracle/product</td>
</tr>
</tbody>
</table>

### PROJECT NAME: CONFIGURATION

<table>
<thead>
<tr>
<th>PROPERTY NAME</th>
<th>VALUE</th>
<th>COMMENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quota</td>
<td>500GB</td>
<td>Quota for the Project including snapshots. The quota should be allocated based on your requirements.</td>
</tr>
<tr>
<td>Mount Point</td>
<td>export/config</td>
<td></td>
</tr>
<tr>
<td>All other settings</td>
<td>Default</td>
<td></td>
</tr>
<tr>
<td>Share Name</td>
<td>aserver</td>
<td>Mounted on apphost1 and apphost2 as /u01/app/oracle/admin/IDMDomain/aserver Contains the domain configuration for the admin server.</td>
</tr>
<tr>
<td>Share Name</td>
<td>mserver_host</td>
<td>One per compute node which runs WebLogic server. Mounted on each application server as /u01/app/oracle/admin/DomainName/mserver Contains the domain configuration for the managed servers. For example: export/config/mserver_apphost1 would be mounted as /u01/app/oracle/admin/DomainName/mserver on apphost1 and export/config/mserver_apphost2 would be mounted as /u01/app/oracle/admin/domainname/mserver on apphost2</td>
</tr>
<tr>
<td>Share Name</td>
<td>oinstance_host</td>
<td>One per compute node which runs a product which uses Oracle_instance for example: Oracle HTTP Server, OID, OVD etc. Mounted on each application server as /u01/app/oracle/admin/Instance_name. Contains the domain configuration for the managed servers.</td>
</tr>
</tbody>
</table>
**PROJECT NAME: TRANSACTIONS**

<table>
<thead>
<tr>
<th>PROPERTY NAME</th>
<th>VALUE</th>
<th>COMMENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quota</td>
<td>200GB</td>
<td>Quota for the Project including snapshots. The quota should be allocated based on your requirements.</td>
</tr>
<tr>
<td>Mount Point</td>
<td>/export/txn</td>
<td></td>
</tr>
<tr>
<td>All other settings</td>
<td>Default</td>
<td></td>
</tr>
</tbody>
</table>
| Share Name    | soa   | Share mount point: /export/txn/soa  
Mounted on apphost1, apphost2 mounted on /u01/app/oracle/admin/soa_cluster.  
Shared location for the JMS  
A directory is created per cluster in the domain and contains sub directories for the JMS and Transaction Log persistent Stores. |

**Snapshot Visibility**

If you are planning on using disk snapshots and wish to be able to access the snapshots directly for the purposes of extracting individual files or backing the snapshot up to tape then project snapshots must be made visible. To do this:

1. Login to the BUI
2. Click on Shares
3. Click on Projects
4. Edit a Project
5. Select Snapshots

**Taking a Backup**

This section of the document describes how to take a backup from a given compute node. When backing up a complete Exalogic machine each compute node will need to be backed up. The procedure is the same for each however.

Most operations can be carried out using the ZFS Storages Appliances’, Browser User Interface (BUI) or the command line utility. To keep things simple this document will only use the BUI.

**Disk Backups**

**Snapshots**

**Scheduling Automatic Snapshots**

Snapshots can be scheduled either through the GUI or via the command line and Open the Browser User Interface (BUI) for the storage head by accessing http://storagenode:215/.
1. Click on Share.
2. Click on Disk Schedules.
3. Click +
4. Enter the following information

<table>
<thead>
<tr>
<th>PROPERTY NAME</th>
<th>VALUE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frequency</td>
<td>Select: half hour, hour, day, week or month</td>
</tr>
<tr>
<td>Offset</td>
<td>Use this to say when the snapshot should be taken, For example Sunday at 02:00hrs</td>
</tr>
<tr>
<td>Keep at most</td>
<td>This is the retention policy. Select how many copies of the snapshot to keep. If an incremental snapshot policy is created then a snapshot will not be deleted until all snapshots that rely on it have been obsoleted.</td>
</tr>
</tbody>
</table>

Ad-hoc Creation

1. A snapshot can be instigated from the BUI by:
2. Click on Snapshots.
3. Select + when list of snapshots is shown.
4. Complete details and hit apply.

Backups using the OS Dump Command

**Dump** examines files on an ext2 filesystem and determines which files need to be backed up. These files are copied to the given disk, tape or other storage medium for safe keeping. A dump that is larger than the output medium is broken into multiple volumes. On most media the size is determined by writing until an end-of-media indication is returned.

An example dump command is:

dump –f mybackupfile filesystems_to_be_backed_up

The dump command can perform leveled backups and the file supplied in the –f switch can be on a remote disk.

For more information on the options available and the further usage of the dump command, see your operating system documentation.

Backups to Remote Disk

**ZFS Server**

ZFS volumes can be replicated to a remote disk array either on demand or as part of a disaster recovery strategy, it does this by creating an implicit snapshot. For Backup/Recovery use case, typically
the remote storage is in the data center and for DR use case it will be in a remote data center. For details on how to set up a disaster recovery strategy, see the white paper

Disaster Recovery for Oracle Exalogic Elastic Cloud.

To replicate a snapshot to a remote ZFS appliance you need to perform the following steps:

1. Login to the BUI using the URL:  https://storageappliance:215/

2. Ensure that the replication service is enabled on both the source and target servers
   i. Select Configuration – Services.
   ii. If the status of the Remote Replication service is not enabled click on the Enable Service button.

3. Create a Replication target.
   i. Click on Remote Replication from Configuration – Services.
   ii. Click on Add Target.
   iii. Enter:
       Name: A name for this target
       Host Name: The Host Name or IP address of the target zfs server
       Root Password: The root password of the target server.
   iv. Click Add

4. Choose which Projects to Replicate.
   i. Click on Shares then the Projects sub-tab.
   ii. Select the project to be replicated and click on Edit Entry.
   iii. Click on the Replication Tab.
   iv. Click on Add.
   v. Enter:
       Target - Select the one created above from the drop down list.
       Select enabled
       Select mode either manual or at selected intervals.

5. You now have the option to schedule replication at pre-defined intervals or manually. To schedule automatically click on Add Entry next to schedule (if you wish to take the backup on an adhoc basis then do not create a schedule).
Enter:

Frequency: The frequency you wish to take a remote backup.
Mins past the hour: The number of minutes past the hour that you wish to take the backup.

6. Click **Add**.

7. Test that replication works by clicking on **Update Now**. Once the backup has taken place, the last Sync field will be populated.

8. Validate that a backup has been taken on the remote server by:
   i. Login to BUI using the URL `https://storageappliance:215/
   ii. Click on **Shares**.
   iii. Click on **Project**.
   iv. Click on the **Replica's** sub tab
   v. You should see the backup you have just taken.
   vi. Now that you have a backup on a remote ZFS appliance, it is possible to mount that backup on a host, which has access to that appliance for the purposes of verification or backing up to tape. This is achieved by performing the following actions on the remote machine.
      Login to the GUI using the URL `https://storageappliance:215/
      Click on **Shares**.
      Click on the **Replica's** sub tab.
      Select the backup and click on **edit entry**.
      Deselect **Inherit from Project**.
      Click on **Export**.
      Choose a mount point.
      Click on **Apply**.
      Mount the file system on the backup host in using an fstab entry similar to:
      ```
      storagehost:/export/product/fmw /u01/app/oracle/product nfs4
      rw,bg,hard,nointr,rsize=131072,wsize=131072
      ```
   vii. Backup to Tape as described in Tape Backups section

**Non-ZFS Server**

If you wish to remotely, backup your data to a remote disk array, which is not running ZFS then:
• Use a NAS Appliance that is connected to the Exalogic Machine via IP-Based protocols using GigE, 10GigE or InfiniBand interfaces.

• If a NAS appliance is not available then it will be necessary to set that appliance up using either NFS or iSCSI, it is not possible to connect directly to a SAN or fibre channel over ethernet. If connecting over NFS performance may be an issue depending on the volume of data being backed up.

• Once the remote disk array is connected to the Exalogic Machine, mount it as a filesystem and then perform backups directly to this filesystem using an operating system command such as tar or dump or any other vendor agnostic file copy utility.

Tape Backups
The following example is based on Oracle Secure Backup, but the principals can be carried over to any media management product. It is possible within Oracle Secure Backup to backup snapshots, however the data volumes in an Oracle Fusion Middleware installation are not large so a standard file system backup is recommended. This will allow the restoration of individual files should the need arise.

This paper does not cover how to install and configure Oracle Secure Backup, except in the context of tasks which need to be performed to achieve a backup of an Exalogic Machine. For example this paper does not include the following tasks all of which you must already have done:

• Installation of Oracle Secure Backup.
• Configuration of the Oracle Secure Backup Domain including, Administration Server, Media Servers and tape devices.
• Media Lifecycle policies such as media families, tape duplication and/or vaulting.

Backing up a file system has six primary configuration elements:

• OSB Client Hosts
• Media Family
• Backup Window
• Datasets
• Backup Schedule and Trigger
• Backup Trigger

These are described in more detail below:

**OSB Client Host**

An Oracle Secure Backup host may be backed up in one of two ways, depending on the host:
1) Traditional backup operation with OSB installed on the host for performing backup of the local file systems (ob access mode)

2) NDMP backup for Network Attached Storage (NAS) devices in which OSB is not installed on the host and instead utilizes NDMP backup/restore (NDMP access mode)

With either method, the host must be configured within the OSB domain.

**OSB Client**

To do this:

1. Login to the OSB GUI using the url https://osbadminserver/
2. Click on the **Configure** tab.
3. Click on the **Hosts** tab.
4. Click **Add**.
5. Enter the following information:
   - **Host**: A name for the host.
   - **IP Interface names, the DNS name or IP address of the host.** (If you have defined a backup network then it will be the DNS Name/IP address of the host on this network).
   - **Roles**: client
   - **Access Method**: ob
   - All other values can be left at the default or changed to match the configuration of your environment.
6. Click **OK**.

**NDMP Client**

To do this:

1. Login to the OSB GUI using the url https://osbadminserver/
2. Click on the **Configure** tab.
3. Click on the **Hosts** tab.
4. Click **Add**.
5. Enter the following information:
   - **Host**: A name for the host.
• IP Interface names, the DNS name or IP address of the storage host. (If you have defined a backup network then it will be the DNS Name/IP address of the storage host on this network).

• Roles: client

• Access Method: NDMP

• User Name / Password. This is the DMA username/password defined in the NDMP service settings of the storage appliance.

• Backup Type – The type of backup you wish to make. Options are zfs, tar or dump.

• All other values can be left at the default or changed to match the configuration of your environment.

6. Click OK.

Media Family

A media family is a logical classification of volumes that share common attributes, for example Retention Periods. So you may wish to create a volume group for each of your volatility groups.

To define a media family in Oracle Secure Backup:

• Login to the OSB GUI using the url https://osbadminserver/

• Click on the Configure tab.

• Click on Add.

• Enter the following information:

  • Name: A name identifying the media family.

  • Volume Expiration: Choose your expiration policy for example if you wish to keep backups for 7 days, select Time Managed and Keep volume for 7 days.

  • Select any other values relevant to your installation and click OK.

Backup Window

A backup window defines a time range within which Oracle Secure Backup (OSB) performs scheduled backup jobs.

For example a backup window could be 1800 – 08:30.

To define a backup window in Oracle Secure Backup:

• Login to the OSB GUI using the url https://osbadminserver/

• Click on the Configure tab.

• Click on the Backup Windows.

• Click on Add.
• Select the type of backup window either Day range or Date, for regular backups Day should be selected.

• If Day range is selected choose the days you want the backup window to apply to. The options are:

  - Daily – Every Day
  - Weekdays – Monday to Friday
  - Weekend – Saturday and Sunday.

• Enter a Local Time Range in the time field, the time is expressed in 24 hr format.

• Click OK to create the backup window.

For the purposes of this document we will create a Daily backup window for the times 02:00 to 06:00.

Datasets

Datasets determine which files are to be backed up; this is done using a lightweight textual language. Datasets can be defined as:

- Inclusions: Files/directories to include in the backup
- Exclusions: Files/directories to omit during the backup

Or a mixture of the two.

The following datasets will be defined:

<table>
<thead>
<tr>
<th>NAME</th>
<th>INCLUSIONS</th>
<th>EXCLUSIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating System</td>
<td>/u01/app/oracle/product/fmw</td>
<td>/u01/app/oracle/admin /u01/app/oracle/txn</td>
</tr>
<tr>
<td>Binaries</td>
<td>/u01/app/oracle/product/fmw</td>
<td></td>
</tr>
<tr>
<td>Configuration</td>
<td>/u01/app/oracle/admin</td>
<td></td>
</tr>
<tr>
<td>Transactions</td>
<td>/u01/app/oracle/txn</td>
<td></td>
</tr>
</tbody>
</table>

Creating a data set in Oracle Secure Backup is achieved by creating a dataset file. A dataset file can be used for a single or multiple compute nodes.
Typically you would create one dataset file for each host you wish to backup. If desired, you could create one for each host/volatility group combination.

**Sample Data Set definitions.**

**Example 1** – Backup /u01/app/oracle/admin on wlshost1

include host wlshost1
include path /u01/app/oracle/admin

**Example 2** – Backup root file system on wlshost1 and wlshost2

include host wlshost1
include host wlshost2

include path /
{
    exclude path /u01/app/oracle/admin
    exclude path /u01/app/oracle/product/fmw
    exclude path /u01/app/oracle/txn
    exclude name core
    exclude name *.bak
}

**Example 3** – Backup /export/config on the storage device using NDMP dump

include host zfsappliance

include path /export/config

**Example 4** – Backup project Domain on the storage appliance using NDMP zfs

You must first determine the ZFS volume name for the project. You can find this information from the zfs BUI.

1. login to BUI.
2. Click on Shares.
3. Click on Projects.
4. Edit the project you wish to backup.
5. On the top of the screen you will see the volume name it will look something like Exalogic/local/ProjectName

**Dataset Example**
Example 5 – Backup Snapshot

include host wlshost1
include path /u01/app/oracle/product/fmw/.zfs/snapshots/mysnapshot

Note: In order to backup the snapshot in this way, the snapshot must be visible, see the Exalogic Disk Layout for details.

Creating the Data Set

To create a dataset file in Oracle Secure Backup

1. Login to OSB GUI
2. Click Backup Tab.
3. Click Datasets.
4. Click Add the new data sets page is displayed.
5. Select Directory from the Dataset Type list
6. Give the Dataset a name.
7. A template data set will be displayed.
8. Edit the data set definition to look like the above, create one for each volatility group.
9. Click Save.
10. Now that the dataset has been created validate it by selecting the dataset and click on Check Dataset.

Backup Schedules and Triggers

A backup schedule is a description of which datasets should be backed up along with any device restrictions.

One or more backup triggers must be created for each backup schedule defining the frequency of backup, backup time and level as well as which media family to employ for the schedule. Based on the backup requirements identified above the following schedule can be put into place:

<table>
<thead>
<tr>
<th>Schedule</th>
<th>Available Times</th>
<th>Data Sets</th>
<th>Level</th>
</tr>
</thead>
</table>

To create a backup schedule in Oracle Secure Backup:

1. Login to Oracle Secure Backup GUI
2. Click on the **Backup** Tab
3. Click **Schedules**.
4. Click **Add** – the New schedule page appears
5. Enter a name for the schedule
6. Enter a priority value for the schedule (If more than one backup schedule is created for the same time they are performed in priority order).
7. Enter the Data Set(s) to include
8. Enter any comments you wish associated with the backup schedule.
9. Click **OK**.

Now that you have defined the backup schedule, you need to specify when you wish it to run. To do this:

1. Login to Oracle Secure Backup GUI
2. Click **Backup**.
3. Click on the **Schedules**.
4. Click on the Backup schedule you created.
5. Click on **Triggers**.
6. Enter:
7. Backup Level – Full or incremental
8. Backup at – Time to start the backup
9. Trigger Type : Day or Month (Select Day for weekly backups)
10. Media Family: Choose which set of tapes to use.
11. Select on which days of the week to perform the backup.
12. Click Add.

Operating System Backups

In an Exalogic Machine the operating system is installed onto local disk, one for each compute node. As the operating system is installed in this way, it cannot be snapshotted or backed up to tape using NDMP. To back up the operating system, you must use either tar or dump for disk, and obtar (the default client backup) for Oracle Secure Backup.

Backup the Switch

The infiniband switches NM2GW and NM2-36P are an integral part of the Exalogic machine configuration and should be backed up along with the operating system. To backup the infiniband switch from the ILOM CLI perform the following steps:

1. Encode the Backup
   
   --> set /SP/config passphrase=\text{\textit{phrase}}
   
   ** The passphrase is any textual password you wish to use to protect the backup **
   
   for example:
   
   --> set /SP/config/passphrase=mypassword1
   
   --> Set ‘passphrase to ‘mypassword1’

2. Backup the configuration
   
   --> set /SP/config dump_uri=\text{\textit{URI}}
   
   Where URL is the command used to perform the backup.
   
   For example
   
   set /SP/config dump_uri=scp://\text{\textit{root}}:\text{\textit{rootpwd}}@123.45.67.89/opt/dump/switch.backup
   
   Where the IP address is the address of the target host for the backup file.
   
   Where /opt/dump/switch.backup is the name of the backup file.
   
   Once the file is onto the file system it can be backed up to more permanent storage as part of the operating system backup.

3. In addition the following files should be backed up to the same location:
   
   /etc/opensm/opensm.conf
• /conf/bx.conf
• /conf/partitions.current

Restoring a Backup

This section shows how to restore the backups you have taken above. There is no provision in this paper for a “bare metal” restore. That is the process of restoring a new machine to the same state as one a backup was taken on. If you need to do this you should first provision the Exalogic Machine using the one command in the usual way. Once you have done this you can then restore the backups you have taken above.

From Disk

Local Snapshots

Snapshots can either be restored in their entirety or individual files can be restored. If you wish to restore an individual file then these can be found in the hidden directory .zfs/snapshot/snapshotname/path_to_file. For example: If you have a project called FMW_Binaries which is mounted on a compute node in the location /u01/app/oracle/product/fmw and you wish to restore a file called /u01/app/oracle/product/fmw/mydir1/myfile from snapshot ADHOC1. Then the backup copy of the file can be found at /u01/app/oracle/product/fmw/.zfs/snapshots/ADHOC1/mydir1/myfile.

If you wish to restore an entire snapshot then this can be restored from the BUI by:

1. Click on Snapshots.
2. Select snapshot and click on restore.

Command Line

Remote Snapshots

To restore from a remote disk backup you must first reverse the direction of replication such that the remote backup is returned to the primary site. You can do this from the BUI as follows:

On the remote machine:

1. Select Shares.
2. Click on Projects sub-tab.
3. Select Replicas.
4. Click on the Replica you wish to restore to the primary machine and click edit.
5. Click on the Replication Sub-tab
6. Click on the Reverse the direction of replication button.
7. You will be prompted to enter a new project name. This is a temporary name, a project will be created on the remote server with this name.

8. Click **Apply**.

9. Click **OK** when you are warned this will stop replication.

10. Click on **Shares**.

11. Click on **Projects**.

12. Find the project you created in 10 above.

13. Click on **Edit**.

14. Click on the **Replication** Sub tab.

15. Click on **Edit**.

16. Select **Include Snapshots** and optionally **SSL**.

17. Click **Apply**.

18. Click on **Update Now** to force the backup to be restored to the primary machine.

At this point, the backup is now back on the primary machine as a replica. It is however not available for use by compute nodes. In order for it to be mountable, you need to do one of two things:

- Clone the Replicated package and then mount the clone.
- Reverse the Replication again. This is the preferred as it not only allows the file system to be mounted again but also reinitiates remote backups.

**On the primary machine:**

First delete the Old project that you are going to recreate.

1. Click on **Shares**.

2. Click on **Projects**.

3. Find the Project you wish to restore and delete it by clicking on the **Remove or destroy entry** next to it.

4. When asked confirm you wish to remove the project.

Now reverse the replication again.

5. Select **Shares**.
6. Click on **Projects** sub-tab.  
7. Select **Replicas**.  
8. Click on the Replica you wish to restore to the primary machine and click edit.  
9. Click on the **Replication** Sub-tab  
10. Click on the **Reverse the direction of replication** button.  
11. You will be prompted to enter a new project name. This is the name of the project you deleted in 3 above.  
12. Click **Apply**.  
13. Click **OK** when you are warned this will stop replication.

At this point, you can remount the project and your backup has been restored. There is one final thing, which needs to be performed, which is to restart the remote backups.

14. Click on **Shares**.  
15. Click on **Projects**.  
16. Find the project you created in 10 above.  
17. Click on **Edit**.  
18. Click on the **Replication** Sub tab.  
19. Click on **Edit**.  
20. Select **Include Snapshots** and optionally **SSL**.  
21. Check that the schedule information is correct, if not edit it until it is satisfactory.  
22. Click **Apply**.  
23. Click on **Update Now** to force a backup and check that replication is once again working.

Stop replication from the primary to the standby.  
From the GUI select the reverse button.

**Dumps**

Dumps are restored using the OS command restore. To use the restore command:

1. Change directory to the root of where you wish the files to be restored to.  
2. To restore the entire backup issue a command similar to:  
   ```
   restore -rf backup_file_name
   ```
To restore individual files or part of the backup issue a command similar to:

```
restore -if backup_file_name
```

This will enter interactive mode where you can chose what files to extract using the add command. Once all files have been selected issue the command extract to restore them.

For more information on the restore command see your operating system documentation.

**From Tape**

If using Oracle secure backup there are three different ways to restore file based backups, this document only covers the catalogue based restore, for details of the other restore types see the Oracle Secure Backup documentation.

A catalogue based restore is achieved by reviewing the objects which have been backed up in the Oracle Secure backup catalogue and then deciding which ones to restore.

To achieve this:

1. Login to the Oracle Secure Backup GUI
2. Click on the Restore Tab.
3. Click on Backup Catalog,
4. Choose a host from the Host Name column
5. Choose the backup you wish to restore from the Data Selector column. The types of backups which can be restored are: Latest/Earliest, backup ID, from a given date.
6. Further narrow the search by adding search options.
7. Enter the path of the files you wish to restore.
8. Click Browse host
9. Once you have determined what you wish to restore click Add.
10. Select the host you wish to restore to (The default is the source host).
11. The restore page is displayed.
12. In the Browse host pane, select the file/directory you wish to restore.
13. Click Add.
14. The restore diagloge page is displayed where you can choose which tape devices to use, and an alternative restore path if desired. When finished click OK.
15. Repeat 12-14 for each file/directory you wish to restore.
16. Click GO to submit the restore job.

Restoring the Switch

Once the switch backup is restored to the filesystem, it can be restored to the switch. This is done via the ILOM CLI using the following steps:

1. Encode the Backup
   
   -> set /SP/config passphrase=\textit{phrase}
   
   Where The passphrase that was used at the time of the backup.
   
   for example:
   
   -> set /SP/config/passphrase=mypassword1
   
   -> Set ‘passphrase to ‘mypassword1’

2. Backup the configuration
   
   -> set /SP/config load_uri=\textit{URI}
   
   Where URL is the command used to perform the restore.
   
   For example
   
   set /SP/config load_uri=scp://root:rootpwd@123.45.67.89/opt/dump/switch.backup
   
   Where the IP address is the address of the target host for the backup file.
   
   Where /opt/dump/switch.backup is the name of the backup file.

3. Manually copy back the following files:
   
   - /etc/opensm/opensm.conf
   - /conf/bx.conf
   - /conf/partitions.current

Conclusion

There are many things to consider when creating a backup strategy including:

- What type of loss (Human or Disaster) are you looking to recover from with your backup strategy?
- What type of Backup technology to use. Disk to Disk or Disk to Tape.
- Object Volatility
- What backup frequency to use.
• What retention policy to implement.

All of these will impact how you implement your backup and recovery strategy. This paper has discussed the various ways of implementing these features and has determined that the best policy to implement, one that caters for both user and machine failure is one that uses a mixture of disk and tape backup technologies:

1. Create disk based snapshots to recover from user errors quickly.

2. Create tape based backups for long term off site archival.

When backing up to tape you have the option of using NDMP or via the compute node. Backing up via NDMP will be faster, and have no overhead on the compute nodes, however it cannot be used to backup the operating system, or any other files, which are stored on local storage. If speed of backup is an issue then the fastest solution would be to use NDMP, however taking the backup from the client maybe more flexible.

Further Reading

• Oracle Exalogic Documentation Library

• Backup and Recovery Performance and Best Practices for Oracle Exadata Cell, and Oracle Exadata Machine.

• Oracle Database Backup and Recovery User’s Guide

• Oracle Secure Backup