Essbase on OCI:
Backup and Restore

This paper covers disaster recovery and version upgrade planning for Essbase instances deployed on OCI.
DISCLAIMER

This document in any form, software or printed matter, contains proprietary information that is the exclusive property of Oracle. Your access to and use of this confidential material is subject to the terms and conditions of your Oracle software license and service agreement, which has been executed and with which you agree to comply. This document and information contained herein may not be disclosed, copied, reproduced or distributed to anyone outside Oracle without prior written consent of Oracle. This document is not part of your license agreement nor can it be incorporated into any contractual agreement with Oracle or its subsidiaries or affiliates.

This document is for informational purposes only and is intended solely to assist you in planning for the implementation and upgrade of the product features described. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described in this document remains at the sole discretion of Oracle.

Due to the nature of the product architecture, it may not be possible to safely include all features described in this document without risking significant destabilization of the code.

1 WHITE PAPER | Essbase on OCI: Backup and Restore | Version 1.2
Copyright © 2020, Oracle and/or its affiliates | Confidential - Public/Oracle Internal/Oracle Restricted/Oracle Highly Restricted
TABLE OF CONTENTS

Disclaimer 1

Purpose Statement 3

Backup and restore terminology and Use cases 3
  Defining Restore Use Cases 3
  Understanding Essbase Backups 4

Use case: Disaster Recovery 5
  Default Essbase Deployment: Recover Compute 5
  Non-Default Essbase Deployment: Recover Compute 10

Essbase Backups: Step-by-step 14
  Backup Entire ATP and Block Volumes: Step-by-Step 14
  Backing up Essbase using Oracle-Provided Scripts 14
  Backing up Essbase using DB client and OCI console 14
  Backup ATP Schema and Block Volumes: Step-by-Step 16
  Before You Begin: Install and Configure Oracle Instant Client and Tools 16
  Backing up Essbase schema using Data Pump and OCI console 18

Various other notes 20
  Managing Volume Groups 20
  Resolving Network Components 20
PURPOSE STATEMENT

This document provides recommendations for the life cycle management of Essbase deployments on Oracle Cloud Infrastructure (OCI). We'll review use cases and steps for full Essbase instance backup in support of disaster recovery and version upgrades. Essbase deployments require regular backup and healthy redundancy planning. For deployments on OCI, block volumes and relational database schemas must be thoughtfully managed.

Application-level backups within an Essbase service also have a very important place in the overall Essbase life cycle management, but they are not the focus of this paper. Here, we are focused on recovering/upgrading the entire Essbase instance (all applications) as of some point-in-time.

Task-level steps described in this whitepaper are as of Essbase version 19.3.0.2.3. Should a step not work exactly as described, please consult the Essbase documentation.

BACKUP AND RESTORE TERMINOLOGY AND USE CASES

When you use the Oracle Marketplace to deploy Essbase on OCI, you don't install it in the traditional sense, as you would to an on-premise server machine. Instead, you deploy Essbase as part of an image on a cloud compute node (or a ‘compute’ for short). This compute, together with the other necessary OCI components (VCN, relational database, block and object storage, etc.), is called an Essbase stack.

Certain components from every stack you create contain information that makes your Essbase deployment unique to your end user community. You will need to back up these unique stack components at appropriate intervals to meet your recovery objectives. In the event of an OCI compute or Availability Domain (AD) failure, you can recover your Essbase instance by building a new stack and restoring into it your Essbase backup. Similarly, you can perform necessary Essbase version updates using backups.

Restore, in this paper, will be a generic term used to describe the action of deploying a new Essbase stack and attaching to it the appropriate block volume and relational database backups.

If your restored Essbase stack should be the latest release, you will use Oracle Marketplace to create it. If you wish to recover the same version of Essbase you ran prior to restoring, then you can take an older deployment script from GITHUB.

Important: Think of the pre-restore Essbase stack as a source (of block volumes, block volume backups, RDB schemas, RDB backups) and the post-restore Essbase stack as a target. Your restored target instance should reflect the source instance as of some point in time.

Defining Restore Use Cases

The restore requirements for your Essbase deployment will define the required backup tasks. There are two common restore scenarios:

Disaster Recovery: should you experience a hardware failure with the compute node in which Essbase is running, you can easily recover your instance in any AD in the same region.

Version Upgrade: between major versions, Oracle will require out-of-place Essbase binary/configuration uptake, esp. when Fusion Middleware changes or Essbase schema changes are being introduced.

Although not every restore use cases is driven by disaster recovery, restoring Essbase always requires the deployment of a new target stack [for the sake of recovering or updating the compute image]. When defining the target stack, you can re-use some source stack components, along with your source backups.

Although not highlighted in this paper, service level agreements (SLAs) with the Essbase user community are an important consideration for restore planning. What is the acceptable downtime window during any recovery or update? There are things you can do to manage the overall time it takes to restore an instance, such as cloning block volumes and building target stacks in advance so that the target OCI environment is in passive standby.

Note: Detailed steps for the version upgrade restore use case will be published with the first major release after 19.3.x.x. The remainder of this paper will focus on disaster recovery.
**Understanding Essbase Backups**

Suitable and reliable backups are the backbone of your restore use case. Any backup of Essbase on OCI will depend on some details of your Essbase stack. A complete backup must protect all information that makes your Essbase deployment unique. These items are:

- Relational database schemas for every Essbase stack, which store some application, user and configuration information.
  - A single database schema for Essbase, called `<instance prefix>_Essbase`
  - Eight database schemas for WebLogic, with the same `<instance prefix>_WebLogic`
- Essbase application and database information stored on a block volume mounted as `/u01/data`. (Essbase is a managed service within a WebLogic domain.)
- WebLogic domain and configuration information stored on a block volume mounted as `/u01/config`. (Essbase is a relational database. Essbase n)

Your backup strategy must ensure that the information above is captured at appropriate intervals to align with your restore use case. Also, the timing of relational database backups and Essbase block volume backups must be synchronized to ensure that the target instance will have the required consistency for Essbase to run properly.

*Consider this*... Although it is possible to restore source block volumes directly to a target stack, you may not know the status of any write operations that were in process in the case of compute disaster recovery. Stopping Essbase before you take a backup allows you to know the exact state of your Essbase data when you use it to restore an Essbase instance.

**Block Volume Backup Planning for Your Restore Use Case**

When you restore Essbase in a target stack, you will always restore and attach a source data block volume backup (and in some cases, a config block volume backup). To consistently restore a target Essbase instance, backups of your source Essbase data block volume

- should be from the same point-in-time as your source ATP database backup.
- should be taken at a time when the Essbase services were stopped.

Optionally, you can work directly with the source block volumes if you are sure about the Essbase data they contain.

Note: Block volumes are restored from backup into an AD of your choosing. Clones can be introduced into your backup processes to minimize Essbase downtime. Block volumes (or clones) cannot be moved between ADs. Clones can be used to quickly replicate a source block volume, then can be backed up and likewise restored into an AD of your choosing. When clones are being used, Essbase must only be stopped during the cloning process.

**Database Backup Planning For Your Restore Use Case**

When you deploy an Essbase stack, the default behavior is to deploy a new ATP database as part of the stack. If you deploy a second Essbase stack in the same region, you can optionally choose to deploy without a second ATP database by selecting the “use existing database” option. This results in license cost savings, as a single ATP database is scalable enough to support schemas for multiple Essbase instances. Schemas associated with each instance of Essbase have a common and unique prefix. The number of Essbase instances deployed in your ATP database, combined with your recovery use case, defines whether you can back up the entire database or if you need to perform schema-level backups.

**Relational Database Backups for Default Essbase Deployments**

Default Essbase deployments consist of a single Essbase stack with RCU schemas deployed into a single relational database. For Essbase default deployments, the relational database can be backed up without exporting schemas for individual Essbase instances. This is possible because restoring the database only impacts one Essbase instance.

**Relational Database Backups for Non-Default Essbase Deployments**

Non-default Essbase deployments consist of multiple Essbase stacks, each with unique RCU schemas, deployed into a single relational database. Essbase non-default deployments require you to refine your relational database backup strategy. Restoration of a relational database backup is “all or nothing”, meaning that the relational database schemas for all Essbase instances would be reset to the same timestamp should a restore action be required on the database.

Best practice for Essbase backups is to synchronize the relational database backup with the block volume backups. But it is not a best practice to require all Essbase instances to be on the same backup and restore schedule. For non-default deployments, isolation of the data and metadata for a single Essbase instance is accomplished by using database schema backups.
Next, we will look at disaster recovery and the backup steps required to support it. Some assumptions have been made to limit the size and scope of this paper. All examples in this paper assume the following:

- ATP is the relational database into which Essbase schemas are deployed
- Oracle Identity Cloud Service (IDCS) is the security provider for the Essbase deployment
- The ESSBASE SYSTEM ADMIN USER NAME (stored in WebLogic – only non-IDCS user in the system) is the same between the source and the target Essbase stack
- The source instance backup has [at the time of restore] at least one valid IDCS user with an Essbase system administrator role.

**USE CASE: DISASTER RECOVERY**

If the compute node on which your Essbase services are deployed fails, you can recover it in any AD in the same region. When you build the target stack and recover the compute, you can re-use many parts of the source stack by using “use existing database” and “use existing network” options. If you have a load balancer in the source deployment, you can change its backend networking and use it with the target stack. You can also attach the block volumes (or their backup/clone) that were previously attached to the source compute.

When restoring your Essbase environment, do not be confused by the term “use existing database”. Although you are free to use a pre-existing relational database, every new Essbase stack will deploy a unique set of Essbase schemas. Deploying into an existing database will not “hook” your target Essbase services to your source Essbase schemas – rather, it will create new target schemas. Mapping source schema data and metadata into the new target database is accomplished when you restore your source database backup into the target.

Remember that a failed compute node will cause failure of your Essbase services. The backups referenced as part of this backup and restore discussion must be taken at regular intervals in advance of any compute failure.

**Default Essbase Deployment: Recover Compute**

Default deployments can be restored from backup using the OCI console.

Backups should be taken prior to compute failure following one of the methods here: [Backup Entire ATP and Block Volumes: Step-by-Step](#). It doesn’t matter whether you choose to backup using Oracle-provided scripts or using a database client and the OCI console.

**1) Deploy a target Essbase stack using Oracle Marketplace**

- Use the source IDCS confidential application
- Use the source ATP database and password
- Use the source VCN and application subnet
- If your source stack has a load balancer, do not deploy a target Load Balancer; you can change the Backend Set after deploying the target stack
- If your source stack has a bastion host, deploy a bastion host with the target stack [source bastion host can be deleted after successful recovery]
- Use the same Essbase system admin user name and password in the target as you used in the source
- Use the same IDCS Essbase admin user in the target stack as you used in the source stack. If this is not possible, make sure the source Essbase instance has at least one valid IDCS user with the Essbase system administrator role.

After you restore, you must login to the target instance as a valid IDCS user who had Essbase system administrator role on the source instance.

The Essbase services in the target stack will be started automatically by the Oracle Resource Manager (ORM) apply job. **Note:** After deploying this stack, two sets of Essbase schemas will be present in your ATP (source and target).

Remember that your ATP backup, taken prior to this stack deployment contains only one set of Essbase schemas (source).
2) **Stop the target Essbase services. [Do not stop the Essbase compute in OCI.]**

*Hint:* It goes without saying that the Essbase services on the `source` compute are stopped, because this use case involves `source` compute hardware failure. If you are simulating these steps, make sure you also stop the `source` compute's Essbase services.

- ssh to the `target` Essbase compute as opc user
- execute the following command: `sudo systemctl stop essbase.service`
  

3) **Restore the source ATP from Backup.**

Be sure to select a `source` ATP backup that was taken during a time when your `source` Essbase services were stopped; also, be sure that you have `source` Essbase ‘data’ and ‘config’ block volumes from the same time.

- Using the OCI console main menu, choose **Autonomous Transaction Processing**
- Select the `source` ATP (note: `source` and `target` schemas are in the `source` ATP)
- Under Resources, select **Backups**
- Find the timestamp of the Backup you want to restore, and select **Restore** using the menu on the right side of the page

*Important:* Before restoring your ATP for the first time, use the following link and carefully review steps 4 and 5. After you complete a restoration of your ATP, you may render other backups invalid, depending on their timestamp.

https://www.oracle.com/pls/topic/lookup?ctx=en/cloud/paas/ftpcloud/id=GUID-78C28C41-AA87-4AD7-EBE6-69325C75F3C

- After the restore finishes, audit your data using a database client like SQL Developer and then be sure to Stop and Start the `source` ATP, which will be in a read only state after a successful restore. You can look at the `ESSBASE_APPLICATION` table within the `<targetprefix>_ESSBASE` schema to verify the restored applications.

4) **Detach ‘data’ and ‘config’ block volumes from the target Essbase compute.**

- As opc user, ssh to your `target` compute and unmount the `/u01/data` volume
  
  `sudo umount /u01/data`

- Using the OCI console main menu, choose **Compute->Instances**
- Select the `target` Compute in which your Essbase instance is deployed
- In **Compute Details->Resources**, select **Attached Block Volumes**
- Using the actions menu to the right of the ‘data’ volume, select **Detach**
- ssh to the `target` Compute as opc user and issue the detach ISCSI commands as indicated.
- Select **Continue Detachment** in OCI after issuing ISCSI detach commands.
- Repeat for the target ‘config’ block volume

https://docs.cloud.oracle.com/en-us/iaas/Content/Block/Tasks/detachingavolume.htm

5) **Create ‘data’ and ‘config’ block volumes from source block volume backup.**

Block volume backups are stored in object storage; they are not able to be attached to compute instances without first creating a new volume in block storage. Clones, on the other hand, are standalone block volumes and can be directly attached to a compute instance. Skip this step if you cloned your block volumes. You may have backed up the block volume group; if so, you can create the volume group.

- Using the OCI console main menu, choose **Block Storage->Block Volume Backups**
- Find the desired ‘data’ volume backup; using the actions menu on the right, select **Create Block Volume**
- Provide a name for the Block Volume and select the correct AD and compartment of your `target` Essbase compute.
- Select **Create Block Volume**
- Repeat for the source ‘config’ block volume backup

https://docs.cloud.oracle.com/en-us/iaas/Content/Block/Tasks/creatingavolume.htm
6) Attach block volumes created in step 5) to the target Compute
   - Using the OCI console main menu, choose Compute->Instances
   - Select the target Compute (the instance you are recovering)
   - Under Resources, select Attached Block Volumes; there should be no attached volumes
   - Select Attach Block Volume
   - Use the default selections for ISCSI, READ/WRITE. Select the correct compartment and then select the source 'data' block volume you just created from backup and select Attach.
   - Repeat for the source ‘config’ block volume you just created from backup
   
   https://docs.cloud.oracle.com/en-us/iaas/Content/Block/Tasks/attachingavolume.htm

7) Connect to newly attached target block volumes and mount them
   - After the restored ‘data’ and ‘config’ volumes are attached to the target compute, use the actions menu for each attached volume to retrieve the ISCSI attach commands.
   - As opc user, connect to the target Compute and execute ISCSI attach commands.
   - As opc user, lsblk to show attached volumes and their disk labels.

   ![lsblk output]

   - As opc user, mount the newly attached volumes as /u01/data and /u01/config
     
     sudo systemctald daemon-reload
     
     sudo mount /dev/sdc1 /u01/config
     
     sudo mount /dev/sdb1 /u01/data
     
     https://docs.cloud.oracle.com/en-us/iaas/Content/Block/Tasks/connectingtoavolume.htm

8) As opc user, update the target compute /etc/fstab file with the UUID of the newly attached ‘data’ and ‘config’ volumes.
   - sudo blkid to show the UUID for the newly attached ‘data’ and ‘config’ block volumes
     
     ![blkid output]
     
     - sudo vi /etc/fstab to update the ‘data’ and ‘config’ lines and replace the UUID, if changed.
9) As opc user, update the target compute /etc/hosts file to map the source domain information to the target

- Determine the domain name of your source compute
- Using the OCI console main menu, choose Resource Manager->Stacks
- Select your source stack to edit its details
- Under Resources->Jobs, select the successful apply job
- Under Job Details->Resources, scroll to the bottom of the log to review the job outputs

```
hostname_host_id = ocidi.instance.oci.pph.aynh+ji3kotfiame+j7haxxx+y1f6fncvqu12kpmf4kmdzg
hostname_host_public_ip = 129.146.203.34
essbase_external_url = https://129.146.88.11/essbase
essbase_node_domain_name = essbaseuckf4ile-1.app.essuckf4ile.oraclelcv.com
essbase_node_id = ocidi.instance.oci.pph.aynh+ji3kotfiamemqwh3nej07kun4ckkmw0ckm64a3jege+nwuf
essbase_node_private_ip = 10.0.1.2
```

- Record the essbase_node_domain_name
- Edit the /etc/hosts file on the target compute and add the source domain information
  
  ```
sudo vi /etc/hosts
```

10) As opc user, update the target compute /etc/oci-hostname.conf file

- Set the PRESERVE_HOSTINFO setting to 3
  
  ```
sudo vi /etc/oci-hostname.conf
```

11) Update source load balancer networking for use with the target compute [skip if no source load balancer]

- Using the OCI console main menu, choose Networking->Load Balancers
- Select the source load balancer
- Select Resources->Backend Sets
- Select the Backend Set essbase
- Select Resources->Backends
- Select Add Backends and select the target compute.
- Remove the Backend corresponding to the source compute

```
<table>
<thead>
<tr>
<th>IP Address</th>
<th>Port</th>
<th>Weight</th>
<th>Drain</th>
<th>Offline</th>
<th>Backup</th>
<th>Health</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.1.4</td>
<td>443</td>
<td>1</td>
<td>false</td>
<td>true</td>
<td>false</td>
<td>green</td>
</tr>
</tbody>
</table>

```

- There is no need to update the IDCS confidential application URLs, as the same load balancer IP is now routing to the target Essbase instance.
12) If your source stack did not have a load balancer, update your IDCS Confidential Application login/logout URLs with the target IP address
   • Login to IDCS and edit the source confidential application to ensure that the target IP address is substituted for the source IP address that was previously used.

13) Start the Essbase services.
   • ssh to the target Essbase compute as opc user
   • execute the following command: sudo systemctl start essbase.service

14) Resolve startup issues, if any.
   • If it takes longer than you expect for Essbase to start, open another bash window to connect and check the status. If you see that the services didn’t find the JDK, then link the source JDK being used by the mounted config volume to the JDK on the target system.

   ```bash
   [opc@essbase26jzoa4p-1 ~]$ sudo systemctl status essbase.service
   [opc@essbase26jzoa4p-1 ~]$ sudo systemctl start essbase.service
   ```

   ```bash
   [opc@essbase26jzoa4p-1 ~]$ sudo ln -s /usr/java/jdk1.8.0_241 /usr/java/jdk1.8.0_221
   ```

   ```bash
   [opc@essbase26jzoa4p-1 ~]$ sudo systemctl status essbase.service
   ```

   ```bash
   [opc@essbase26jzoa4p-1 ~]$ sudo systemctl status essbase.service
   ```

   • Link the source JDK to the JDK the target is expecting

   ```bash
   [opc@essbase26jzoa4p-1 ~]$ sudo ln -s /usr/java/jdk1.8.0_241 /usr/java/jdk1.8.0_221
   ```

   ```bash
   [opc@essbase26jzoa4p-1 ~]$ sudo systemctl status essbase.service
   ```

   ```bash
   [opc@essbase26jzoa4p-1 ~]$ sudo systemctl status essbase.service
   ```

   • Print the following command: sudo systemct start essbase.service in the 2nd bash window

---

Copyright © 2020, Oracle and/or its affiliates | Confidential - Public/Oracle Internal/Oracle Restricted/Oracle Highly Restricted
15) After successfully recovering into the target Essbase stack, you can delete the failed source compute node and do further cleanup to un-needed block volumes and backups.

Non-Default Essbase Deployment: Recover Compute

Remember that non-default deployments have schemas for multiple Essbase instances in a single ATP. Still, if a compute failure takes place for one of the Essbase instances, you will deploy the new target Essbase schemas in the same ATP. You will then use relational database schema backups to import the source Essbase schema into the target. Source continues to refer to the schema belonging to the failed Essbase compute node, and target refers to a newly deployed stack built with “use existing database” and “use existing VCN” options.

Before beginning this recovery, backups should be taken following this method: Backup ATP Schema and Block Volumes: Step-by-Step. To perform schema backups using data pump, you will need to first install and configure the Oracle Instant Client.

1) Deploy a target Essbase stack using Oracle Marketplace

- Use source IDCS confidential application
- Use source ATP database and password
- Use source VCN and application subnet
- If your source stack has a load balancer, do not deploy a target Load Balancer -- you can change the Backend Set after deploying the target stack
- If your source stack has a bastion host, deploy a bastion host with the target stack [source bastion host can be deleted after successful recovery]
- Use the same Essbase system admin user name and password in the target as you used in the source
- Use the same IDCS Essbase admin user in the target stack as you used in the source stack. If this is not possible, make sure the source Essbase instance has at least one valid IDCS user with the Essbase system administrator role. After you restore, you must login to the target instance as a valid IDCS user who had Essbase system administrator role on the source instance.

The Essbase services in the target stack will be started automatically by the ORM apply job.

Note: After deploying this stack, you will have one additional set of Essbase schemas in your ATP, because the failed instance has both source and target schemas. After completing the recovery, you can drop the schemas from the failed source instance.

2) Stop the target Essbase services. [Do not stop the Essbase compute in OCI.]

Hint: It goes without saying that the Essbase services on the source compute are stopped, because this use case involves source compute hardware failure. If you are simulating these steps, make sure you also stop the source compute’s Essbase services.

- ssh to the target Essbase compute as opc user
- execute the following command: sudo systemctl stop essbase.service

3) Restore the target ATP Schema from source Schema Backup.

When restoring the ATP for your target stack, you will import your source schema backup into the target Essbase schema using the REMAP_SCHEMA option.

Be sure to select a source schema backup that was taken during a time when your source Essbase services were stopped; also, be sure that you have source Essbase ‘data’ block volume from the same time. In the case of compute recovery for non-default deployments, we will not replace the target ‘config’ block volume.

Note: the ATP will already be configured for use with object storage

- Make sure your instant client is configured to point to the ATP containing your source and target Essbase schemas
- Using the Oracle instant client, issue the following data pump import command
After the schema import finishes, audit your data using a database client like SQL Developer. You can look at the ESSBASE_APPLICATION table within the <targetprefix>_ESSBASE schema and see that the target schema (which was empty prior to schema import) has the source applications.

4) Detach ‘data’ block volume from the target Essbase compute.

- As opc user, connect to your target compute and unmount the /u01/data volume
  
  
  
  
  
  sudo umount /u01/data

- Using the OCI console main menu, choose Compute->Instances
- Select the target Compute in which your Essbase instance is deployed
- In Compute Details->Resources, select Attached Block Volumes
- Using the actions menu to the right of the ‘data’ volume, select Detach
- ssh to the Compute as opc user and issue the detach ISCSI commands as indicated.
- Select Continue Detachment in OCI after issuing ISCSI detach commands.

https://docs.cloud.oracle.com/en-us/iaas/Content/Block/Tasks/detachingavolume.htm
5) **Create ‘data’ block volume from source block volume backup.**

Block volume backups are stored in object storage; they are not able to be attached to compute instances without first creating a new volume in block storage. Clones, on the other hand, are standalone block volumes and can be directly attached to a compute instance. Skip this step if you cloned your block volumes. You may have backed up the block volume group; if so, you can create the volume group.

- Using the OCI console main menu, choose Block Storage->Block Volume Backups
- Find the desired ‘data’ volume backup; using the actions menu on the right, select Create Block Volume
- Provide a name for the Block Volume and select the correct AD and compartment of your target Essbase compute.
- Select Create Block Volume

https://docs.cloud.oracle.com/en-us/iaas/Content/Block/Tasks/creatingavolume.htm

6) **Attach ‘data’ block volume created in step 5) to the target Compute**

- Using the OCI console main menu, choose Compute->Instances
- Select the target Compute (the instance you are recovering)
- Under Resources, select Attached Block Volumes; there should be no attached ‘data’ volume
- Select Attach Block Volume
- Use the default selections for ISCSI, READ/WRITE. Select the correct compartment and then select the source ‘data’ block volume you just created from backup and select Attach.

https://docs.cloud.oracle.com/en-us/iaas/Content/Block/Tasks/attachingavolume.htm

7) **Connect to newly attached target block volume and mount it**

- After the restored ‘data’ volume is attached to the target compute, use the actions menu for each attached volume to retrieve the ISCSI attach commands.
- As opc user, connect to the target Compute and execute ISCSI attach commands.
- As opc user, `lsblk` to show attached volumes and their disk labels.

```
[opc@essbase26 /]$ lsblk
NAME       MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
sdb         8:16   0  1024G  0 disk          
sdb1        8:17   0  512G   0 part [swap]    
sdc         8:32   0  512G   0 part          
sdc1        8:33   0  512G   0 part          
sda         8:0    0  46.6G   0 part [swap]   
sda2        8:1    0  38.4G   0 part          
sda3        8:2    0  208M   0 part          
```

- As opc user, mount the newly attached volume as `/u01/data`

```
sudo systemctl daemon-reload
sudo mount /dev/sdb1 /u01/data
```

https://docs.cloud.oracle.com/en-us/iaas/Content/Block/Tasks/connectingtoavolume.htm

8) **As opc user, update the target compute `/etc/fstab` file with the UUID of the newly attached ‘data’ volume.**

- `sudo blkid` to show the UUID for the newly attached ‘data’ block volume

```
[/dev/sdb1]: UUID="58b0f6c9-5eb3-43f8-95e6-de65c6f35fcf" TYPE=ext4 PARTUUID="52263590-157a-4c4a-a9d8-8253c7332112"
[/dev/sdb1]: UUID="498e02c9-8301-44fc-8c9c-259c53777777-427a-a35c-9b9c0b650f83" TYPE=ext4 PARTUUID="f75c8e9f-7777-427a-a35c-9b9c0b650f83"
[/dev/sdb1]: UUID="84ff20b0-8301-44fc-8c9c-259c53777777-427a-a35c-9b9c0b650f83" TYPE=ext4 PARTUUID="f75c8e9f-7777-427a-a35c-9b9c0b650f83"
```

- As opc user, update the target compute `/etc/fstab` file with the UUID of the newly attached ‘data’ volume.
sudo vi /etc/fstab to update the ‘data’ line and replace the UUID, if changed.

9) Update source load balancer networking for use with the target compute [skip if no source load balancer]
   - Using the OCI console main menu, choose Networking->Load Balancers
   - Select the source load balancer
   - Select Resources->Backend Sets
   - Select the Backend Set essbase
   - Select Resources->Backends
   - Select Add Backends and select the target compute.
   - Remove the Backend corresponding to the source compute.

   There is no need to update the IDCS confidential application URLs, as the same load balancer IP is now routing to the target Essbase instance.

10) If your source stack did not have a load balancer, update your IDCS Confidential Application login/logout URLs with the target IP address
    - Login to IDCS and edit the source confidential application to ensure that the target IP address is substituted for the source IP address that was previously used.

11) Start the Essbase services.
    - ssh to the target Essbase compute as opc user
    - execute the following command: sudo systemctl start essbase.service

12) After successfully recovering source information into the target Essbase stack, you can delete the failed source compute node and do further cleanup to un-needed block volumes and backups. At this time, you can also drop the failed source schemas from your ATP.
**ESSBASE BACKUPS: STEP-BY-STEP**

Essbase backups support your recovery needs. Depending on your recover use case, you will follow one of two backup methods. They differ in the treatment of the relational database backup. Sometimes you will restore the entire relational database, and at other times, you will restore only selected schemas from the relational database. The restore use cases above indicate which backup method to follow.

**Backup Entire ATP and Block Volumes: Step-by-Step**

If your default deployment uses Autonomous Transaction Processing (ATP) as the relational database, then you can use Oracle-provided scripts to take synchronized backup of your ATP and Essbase block volumes. Alternatively, you can use a database client and the OCI console to perform the same steps. If you deployed using DBaaS, then you must take manual backups, but the concepts for when to use the full database vs schema backup apply to the various ‘restore’ use cases.

**Backing up Essbase using Oracle-Provided Scripts**

Backup scripts are provided for default Marketplace deployments that use ATP as the relational database. The provided scripts perform the following tasks:

1. **Configure your ATP to work with your object storage**
2. **Stop the Essbase services**
3. **Back up your ATP**
4. **Back up your Essbase ‘data’ and ‘config’ block volumes**
5. **Start the Essbase services**

To initiate a backup of an instance created using the default Marketplace image deployment, schedule the backup for a convenient time when your users are not in the system and follow these steps:

- Using documentation, ensure that the required policies to manage backups are in place
  https://www.oracle.com/pls/topic/lookup?ctx=en/database/other-databases/essbase/19.3&id=GUID-64D56F3C-ED1A-4CF4-8CF7-AACB669EBB87
- ssh to your Essbase compute as opc user (If you deployed a Bastion host, you will use it as a proxy)
- cd /u01/vmtools
- ./configure-backup-storage.sh
- ./backup.sh
- Note: Essbase services will automatically be stopped and started by the backup.sh script.

**Backing up Essbase using DB client and OCI console**

Alternatively, you can use a database client and the OCI console to perform backups of Essbase default Marketplace deployments. Remember that an Essbase backup consists of block volume backups and ATP backup.

1. **Configure your ATP instance to work with your object storage**

   Use a DB client application to configure your ATP instance for use with your OCI account and a default object storage bucket. SQL Developer is a nice choice for DB client, because it allows Cloud Wallet connections and can connect to multiple ATP instances at the same time, if needed.

   - Create a connection to your ATP instance using SQL Developer [consider your proxy needs if connected via a corporate network – not described here]:
     - Database Type Oracle
     - Authentication type Default
     - Username admin
     - Password [database password you provided during Essbase deployment]
     - Connection Type Cloud Wallet
     - Configuration File [Browse to location of downloaded ATP wallet .zip file]
     - Service [select the _low service for your ATP wallet]


   - Create an auth token using the OCI Console.
Identity->Users->User Details->Auth Tokens->"Generate Token"

Copy and record the token value in a secure location. You will not be able to retrieve it again.

https://docs.cloud.oracle.com/en-us/iaas/Content/Registry/Tasks/registrygettingauthtoken.htm

- Using SQL Developer, connect to your ATP instance and execute the following SQL:
  i) Create cloud credential to identify your OCI user
      BEGIN
        DBMS_CLOUD.CREATE_CREDENTIAL(
          credential_name => '<name of you choosing>',
          username => '<your OCI username>',
          password => '<OCI auth token value>'
        );
      END;
  ii) Associate the cloud credential with your ATP instance
      ALTER DATABASE PROPERTY SET DEFAULT_CREDENTIAL = 'ADMIN.<credential_name from above>';
  iii) Set the default OCI Object Storage Namespace for your ATP database
      ALTER DATABASE PROPERTY SET default_bucket='https://swiftobjectstorage.us-phoenix-1.oraclecloud.com/v1/idpzbwwxxxxmy';

      Note: us-phoenix-1.oraclecloud.com should be replaced with your OCI region
      Note: idpzbwwxxxxmy should be replaced with the Namespace of your object storage.
      https://docs.cloud.oracle.com/en-us/iaas/Content/Object/Tasks/understandingnamespaces.htm


2) Stop the Essbase services. [Do not stop the Essbase compute in OCI.]
   - ssh to the Essbase compute as opc user
   - execute the following command: sudo systemctl stop essbase.service

3) Back up your ATP
   - In the OCI console, navigate to the details of your ATP instance.
   - Select Backups from the lower left, then Create Manual Backup.
   - Provide a Name for the backup and click Create.

   Your backup is automatically stored in the default object storage space for your ATP instance.

4) Backup your Essbase ‘data’ and ‘config’ block volumes
   - In the OCI console, navigate to Block Storage->Block Volume Groups
   - Find the volume group that corresponds to your Essbase compute (use of optional RESOURCE DISPLAY NAME PREFIX
     when creating your stack allows you to identify all stack components using a common prefix)
   - Using the actions menu to the right of the created date, select Create Volume Group Backup
   - Provide a Name for the backup group and click Create.
   - Alternatively, you can create a clone of the volume group. Read about backups and clones here:
     https://docs.cloud.oracle.com/en-us/iaas/Content/Block/Concepts/blockvolumebackups.htm

5) Start the Essbase services.
   - ssh to the Essbase compute as opc user
   - execute the following command: sudo systemctl start essbase.service

6) Note the timestamp of your ATP and Block Volume backups. Because your Essbase services are stopped, these
   backups can be used to consistently restore Essbase if the need arises.
Backup ATP Schema and Block Volumes: Step-by-Step

Before You Begin: Install and Configure Oracle Instant Client and Tools

Backing up non-default Marketplace deployments requires use of the Oracle Database Instant Client and Oracle Data Pump to export the schemas related to a specific Essbase instance instead of taking a complete ATP backup. The Oracle Database Instant Client is recommended for this purpose.

1) Download and install an Instant Client version compatible with your ATP version. Oracle Instant Client

Downloads

- Essbase 19c deployments recently began using ATP version 19c. [The examples in this paper were created with ATP version 18c.]
- Be sure to download and install the corresponding Visual Studio Redistributable
- You will also need the Tools Package which includes Data Pump
- Optionally, you can download SQL*Plus Package, but SQL developer will work as well.
- See the installation instructions on the platform install download page for the installation steps required after you download Oracle Instant Client and the Tools Package. Below is an example:

```
Instant Client installation for Microsoft Windows 64-bit

See the Instant Client Home Page for more information about Instant Client packages.
Client-server version interoperability is detailed in Doc ID 2075783.1 For example, Oracle Call Interface 19, 18 and 12.2 can connect to Oracle Database 11.2 or later. Some tools may have other restrictions.
1. Download the appropriate Instant Client packages for your platform. All installations require the Basic or Basic Light package.
2. Unzip the packages into a single directory such as C:\oracle\instantclient_19_6
3. Add this directory to the PATH environment variable. If you have multiple versions of Oracle libraries installed, make sure the new directory occurs first in the path. Restart any terminal windows or otherwise make sure the new PATH is used by your applications.
5. If you intend to co-locate optional Oracle configuration files such as tnsnames.ora, sqlnet.ora, ldap.ora, or oraaccess.xml with Instant Client, then create a subdirectory such as C:\oracle\instantclient_19_6\nvrock\admin
   This is the default Oracle client configuration directory for applications linked with this Instant Client.

   Alternatively, Oracle client configuration files can be put in another, accessible directory. Then set the environment variable TNS_ADMIN to that directory name.

6. Start your application.

ODBC users should follow the ODBC installation instructions.
```
2) Configure your Instant Client for use with multiple ATP instances:

- Download the DB Wallet from each ATP instance you plan to connect to.

- Create a network folder under your instant client folder; for example, C:\temp\instantclient_18_5\network

- Unzip the wallet contents for each ATP instance in a folder under your network folder; for example:

```
<table>
<thead>
<tr>
<th>Name</th>
<th>Date modified</th>
<th>Type</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>owallet.sso</td>
<td>4/3/2020 6:44 PM</td>
<td>SSO File</td>
<td>7 KB</td>
</tr>
<tr>
<td>owallet.p12</td>
<td>4/3/2020 6:44 PM</td>
<td>Personal Information...</td>
<td>7 KB</td>
</tr>
<tr>
<td>keystore.jks</td>
<td>4/3/2020 6:44 PM</td>
<td>JKS File</td>
<td>4 KB</td>
</tr>
<tr>
<td>${jdbc.properties}</td>
<td>4/3/2020 6:44 PM</td>
<td>PROPERTIES File</td>
<td>1 KB</td>
</tr>
<tr>
<td>readme.md</td>
<td>4/3/2020 6:44 PM</td>
<td>MD File</td>
<td>1 KB</td>
</tr>
<tr>
<td>sqlnet.ora</td>
<td>4/3/2020 7:05 PM</td>
<td>ORA File</td>
<td>2 KB</td>
</tr>
<tr>
<td>tnsnames.ora</td>
<td>4/3/2020 6:44 PM</td>
<td>ORA File</td>
<td>2 KB</td>
</tr>
<tr>
<td>truststore.jks</td>
<td>4/3/2020 6:44 PM</td>
<td>JKS File</td>
<td>4 KB</td>
</tr>
</tbody>
</table>
```

- Edit the sqlnet.ora file for each unzipped wallet folder and update the WALLET_LOCATION:

```
[oracle@temp instantclient_18_5]$ vi sqlnet.ora
```

- Set a system environment variable appropriate for your instant client install location

```
TNS_PATH= C:\temp\instantclient_18_5\network
```

- When you are ready to connect to an ATP instance using the Instant Client, SET/EXPORT a TNS_ADMIN variable for your shell (examples in this document use bash on windows); then connect.

```
$ export TNS_ADMIN=$TNS_PATH/<unzipped wallet folder name>

$ sqlplus admin@<"ATP wallet TNS connection"_low>
```

```
krutzekrutzekatl /usr/bin
$ export TNS_ADMIN=$TNS_PATH/embWL_admin/

krutzekrutzekatl /usr/bin
$ sqlplus admin@ess8frzlime_low

SQLPlus: Release 18.0.0.0.0 - Production on Fri Apr 3 20:16:40 2020
Version 18.5.0.0.0

Copyright (c) 1982, 2018, Oracle. All rights reserved.

Enter password:
Last Successful login time: Fri Apr 03 2020 20:13:58 -07:00
Connected to:
Oracle Database 18c Enterprise Edition Release 18.0.0.0 - Production Version 18.4.0.0

SP2-0318: unable to open file "LOGIN.SQL"
```
Backing up Essbase schema using Data Pump and OCI console

1) Configure your ATP instance to work with your object storage

Same as Backing up Essbase using DB client and OCI console, step 1). Or, optionally, you can use SQL*Plus and Oracle Instant Client.

2) Stop the Essbase services. [Do not stop the Essbase compute in OCI.]

Same as Backing up Essbase using DB client and OCI console, step 2).

3) Backup the Essbase schema from your ATP instance using Data Pump and move the .dmp file to OCI Object Storage

Each Essbase instance has 9 associated schemas in your ATP. All 9 schemas have a common rcu_schema_prefix, which is reported in the outputs of the Oracle Resource Manager (ORM) apply job. When using IDCS for security, you only need to back up the <prefix>_ESSBASE schema that corresponds to the Essbase instance you want to back up. Remember that your ATP instance may have Essbase schemas from multiple instances.

- Make sure your TNS_ADMIN variable points to the wallet location of the ATP instance you plan to export from. Use Oracle Instant Client to issue the following Data Pump command:

  $ export TNS_ADMIN=TNS_PATH/mywallet_admin

  $ expdp admin/E55base2020##@ESSOT8QU27W_low directory=data_pump_dir schemas=ESSHE4U6C90__ESSBASE logfile=ESSHE4U6C90.out dumpfile=ESSHE4U6C90.dmp

  Note that the ATP prefix in the connection information may not be the same as the schema prefix for the Essbase schema you are backing up.

- Schema backups are physically stored on disk in the Data Pump Directory of your ATP.
- Move the .dmp file into an Object Storage bucket of your choosing (use SQL Developer, unless you installed the Instant Client SQL*Plus package). The /o/xxxxxxxxxx.dmp portion of the PUT_OBJECT uri indicates the name you want to assign for the .dmp file in your Object Storage. The file_name must match the .dmp filename you assigned when you created the export on disk using data pump.

```
BEGIN
  DBMS_CLOUD.PUT_OBJECT(credential_name => 'DEF_CRED_kz',
                        object_uri => 'https://objectstorage.us-phoenix-1.oraclecloud.com/n/idpbzw1f44my/b/backup_essot8qu27w/o/essbaseschema_ESSHE4U6C90.dmp',
                        directory_name => 'DATA_PUMP_DIR',
                        file_name => 'ESSHE4U6C90.dmp');
END;
/
```

- Refresh your Object Storage Bucket to see the dmp file.

4) **Backup the Essbase ‘data’ and ‘config’ block volumes**
   Same as [Backing up Essbase using DB client and OCI console](#) step 4). [Make sure you back up the block volumes attached to the Essbase instance for which you just exported RCU schemas.]

5) **Start the Essbase services.**
   Same as [Backing up Essbase using DB client and OCI console](#) step 5).

6) **Note the timestamp of your ATP .dmp file in object storage and block volume backups.** Because your Essbase services were stopped, these backups can be used to consistently restore Essbase if the need arises.
VARIOUS OTHER NOTES

Managing Volume Groups
After detaching and attaching volume groups, you may want to perform some maintenance to ensure that the ‘config’ and ‘data’ volumes running in your target Essbase instance are so-called “matched pairs”.

You can use the OCI console to manage Block Volume Groups.

- Select the Block Volume Group for your target Essbase instance.
- Remove any Block Volumes in the group that are no longer attached to your compute.
- Add Block Volumes that are not in the group but are attached to your compute.

Resolving Network Components
To minimize disruption to your end user community, you should consider the use of some resolving network component to maintain a consistent URL endpoint for your users. You should work with your networking team to assign an appropriate corporate domain endpoint for your Essbase instance(s).

On a Windows box, this can be simulated as follows:

- **As an administrator**, edit the `Windows\System32\drivers\etc\hosts` file, adding your target IP address and some domain name (essbase.com)

```plaintext
# This is a sample hosts file used by Microsoft Windows.
# This file contains the mappings of IP addresses to host names. Each entry should be kept on an individual line. The IP
# address should be placed in the first column followed by the corresponding host name. The IP address and the host name
# should be separated by at least one space.
# Additionally, comments (such as those) may be inserted on individual lines or following the machine name denoted by a '#'
# symbol.
# For example:
10.54.94.97    chinonome.com  # source server
30.25.62.10    k.ename.com  # a client host

# localhost name resolution is handled within DNS itself.
localhost       127.0.0.1

# Loopback interface
127.0.1.1

192.168.30.177  essbase.com
```

- Edit your target IDCS application and replace the IP address with the domain you used above.

- Connect to Essbase using the modified essbase_external_url from your apply job output.
If you are using Essbase version 19.3.0.0.1, there are additional steps to those directly above.

1) **Connect to your compute as opc user**
2) **Edit auth_openidc_essbase.conf**
   
   ```bash
   sudo vi /etc/httpd/conf.d/auth_openidc_essbase.conf
   ```
   
   search for your load balancer IP and replace it with your domain name [example: essbase.com]
3) **Add your domain name to /etc/hosts**
   
   ```bash
   sudo vi /etc/hosts
   ```
   
   add a line with load balancer IP and your domain name
4) **Update /etc/oci-hostname.conf**
   
   ```bash
   sudo vi /etc/oci-hostname.conf
   ```
   
   change PRESERVE_HOSTINFO setting to 3 (to retain changes to /etc/hosts)
5) **Restart httpd:**
   
   ```bash
   sudo systemctl restart httpd
   ```
Esbase on OCI: Backup and Restore
September, 2020
Author: Karen Zubetz