

RMAN Compression and Encryption:

RMAN Compression (Optional)	RMAN Encryption (Mandatory)
<ul style="list-style-type: none">- 10g: BASIC- 11g and above: HIGH, BASIC, MEDIUM,LOW- MEDIUM recommended- <u>No ACO licensing required</u> <p>CONFIGURE COMPRESSION ALGORITHM 'MEDIUM';</p> <p>BACKUP AS COMPRESSED BACKUPSET DATABASE PLUS ARCHIVELOG;</p>	<ul style="list-style-type: none">- Password, Transparent Data Encryption (TDE), Dual-Mode- <u>No ASO licensing required</u>- Keys are kept local (not in the storage cloud)- If TDE is used (preferred), then simply use SET ENCRYPTION ON before backups and restores- For password encryption: SET ENCRYPTION ON IDENTIFIED BY '<password>' ONLY;- Before doing restore, SET DECRYPTION IDENTIFIED BY '<password>';

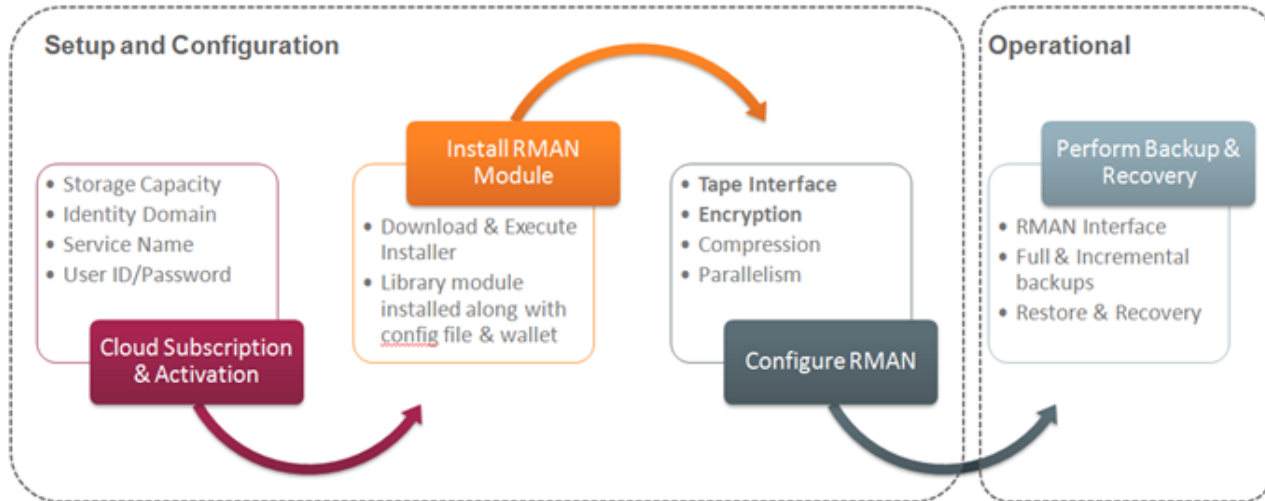
Setting up Oracle Database Backup Cloud Service in simple 4 steps.

1. Subscribe for the Oracle Database Backup Cloud Service. You can do that from shop.oracle.com (or) work with your Oracle representative. Alternatively, you can choose to give it a try using Database Cloud Service trial. For more information, refer to cloud.oracle.com/database_backup.
2. Download and install the Oracle Database Cloud Backup Module from Oracle Technology Network (OTN). The module is what makes it possible to perform secure cloud backups and restores. You'll install the module on the system where your Oracle database is running. Multiple database versions and operating systems are supported.
3. After you install the backup module, you'll configure a few RMAN settings.
4. Then you're ready to perform backup & recovery operations to the cloud using familiar RMAN commands.

You'll use the online dashboard to monitor your service and see how much storage capacity you're using for your backups..

*-These procedures will change when the Recovery Appliance is the backup destination.

High Level Architecture of Oracle Cloud Backup



Cloud Backup Module

The module is a system backup to tape (SBT) interface that's tightly integrated with Recovery Manager (RMAN), which means you don't need to learn new tools or commands.

You can continue to use standard RMAN commands for all backup, restore, recovery, and maintenance operations

You'll download the backup module from Oracle Technology Network (OTN) and install it on your database server. Multiple database versions and operating systems are supported. For more information about the module, see [Installing the Oracle Database Cloud Backup Module](#).

Workflow:

1. RMAN streams backup data to the cloud via RMAN cloud module
2. Cloud module breaks backup pieces into 100MB chunks (Default) and ships to the cloud
 - a. Failed transmissions are retried automatically.
 - b. Multiple buffers (RMAN Channels) can be used for parallelism and to increase backup throughput if there is sufficient network bandwidth.
3. Each chunk is stored as an object inside the Oracle clouduser container. The container can either be user pre-created (or) automatically created by the RMAN cloud module. Default container name : "oracle-data-[first 8 chars of service & domain]"
4. Uses REST API calls – PUT, GET, POST, HEAD & DELETE over HTTPS
5. Typical URL formation for every object
 - a. `http://<identitydomain>.storage.oraclecloud.com/v1/<service>-<domain>/<container>/<piece name>/<unique ID>/0000001, 0000002 ..`
 - b. Creates and maintains metadata XML files in the cloud which acts as manifest files and used by the RMAN module.

*-These procedures will change when the Recovery Appliance is the backup destination.

Required Configuration Files for Cloud Backups

File name	Location / Creation	Purpose
libopc.so(or) oraopc.dll	User specified library location. Downloaded by the installer.	SBT library which enables backup to Oracle Cloud
opc<SID>.ora	Configured by the installer under \$ORACLE_HOME/dbs	Contains ODBS container URL location for the user and also the ODBS credential wallet location
cwallet.sso	User specified wallet location during the RMAN module installation.	Oracle wallet which securely stores backup service credentials. This is used during RMAN backups and restore operations .
Wallet for encryption (optional –only needed for TDE)	Either \$ORACLE_BASE /admin/\$ORACLE_SID /wallet (or) defined in sqlnet.ora / Existing wallet	Used for backup encryption. Existing Oracle wallet can be used (or) new Oracle wallet can be created.

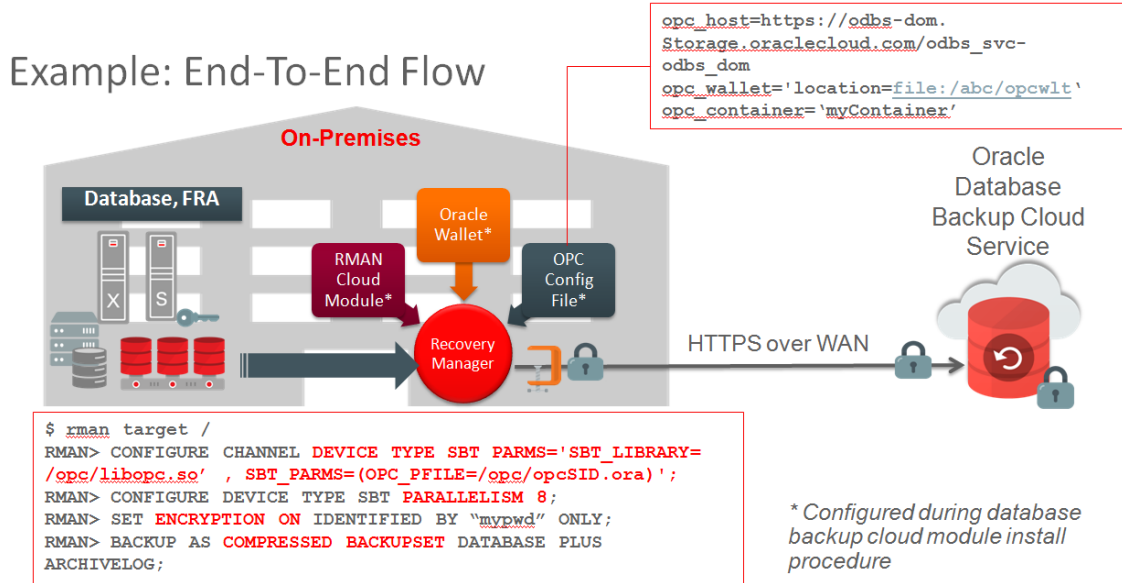
Content of the OPC Configuration File - Run time configurations (located under \$ORACLE_HOME/opc<sid>.ora)

Parameter Name	Description
OPC_HOST	REST destination URL <u>Ex:</u> https://mydomain.storage.oraclecloud.com/v1/my-service-mydomain
OPC_WALLET	OPC credential wallet location Ex: 'LOCATION=file://home/oracle/OPC/wallet CREDENTIAL_ALIAS=odbs_opc'
OPC_CONTAINER	User specified container name Ex:PAYROLL_DB (Customer need to create that using tools like cloudberry until Oracle Cloud has GUI)
OPC_CHUNK_SIZE	Specified in bytes. By default, 100MB. Not recommended to change.
_OPC_TRACE_LEVEL	For debug purposes only. Set this parameter to – say 100 which generates more trace information in sbtio.log.

*-These procedures will change when the Recovery Appliance is the backup destination.

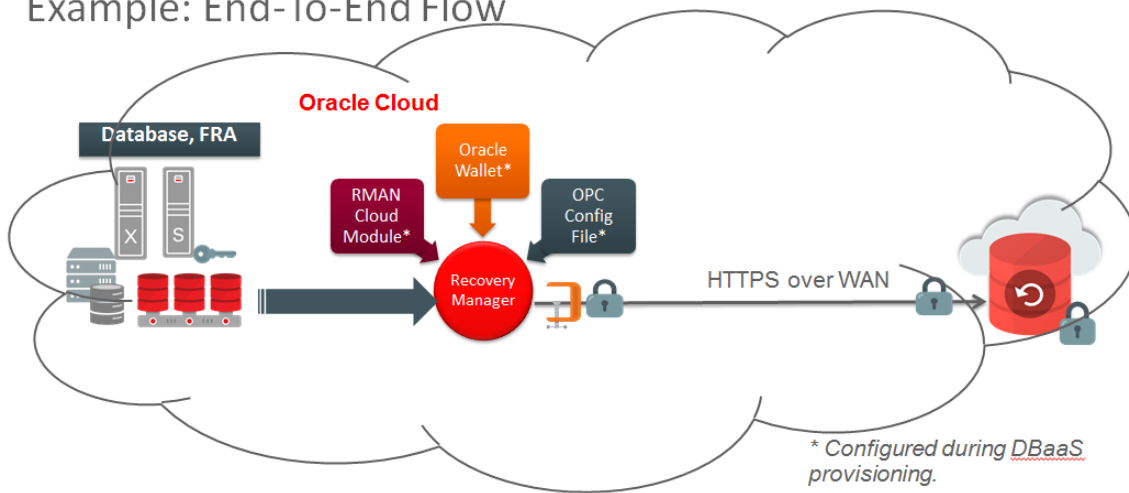
Architecture of Oracle Cloud Backup when used with On-Premise Databases

Example: End-To-End Flow



Architecture of Oracle Cloud Backup when used with Cloud Deployed Databases

Example: End-To-End Flow



*-These procedures will change when the Recovery Appliance is the backup destination.

Oracle Database Backup Cloud Service: Best Practices

In this section we will discuss the best practices when backing-up or recovering to or from the Oracle Cloud Backup Service. These best practices are based on native RMAN commands.

Before you start, ensure you have installed the Oracle Cloud Backup module from OTN and you configure your RMAN environment properly.

```
RMAN>CONFIGURE CHANNEL DEVICE TYPE 'SBT_TAPE' PARMS  
'SBT_LIBRARY=/home/oracle/OPC/lib/libopc.so,  
ENV=(OPC_PFILE=/u01/products/db/12.1/dbs/opcodbs.ora)';
```

Backup

- **RMAN encryption for backups is enforced (mandatory for On-Premise Databases)**

- Use the RMAN set encryption clause in your RMAN run block.

```
RMAN> SET ENCRYPTION ON IDENTIFIED BY 'abc123' ONLY;
```

Keys are managed by the customer (password, TDE, dual-mode)

Data securely transmitted to the cloud over HTTPS

- **To optimize data transfer when network bandwidth is limited and CPU resources are available**

- Use RMAN compression (HIGH, MEDIUM, LOW, BASIC)

```
RMAN> CONFIGURE COMPRESSION ALGORITHM 'MEDIUM';
```

```
RMAN>BACKUP DEVICE TYPE SBT AS COMPRESSED BACKUPSET DATABASE PLUS ARCHIVELOG  
FORMAT '%d_%U';
```

- Increase PARALLELISM (until you reach acceptable network throughput or hit max throughput capable with the existing network)

```
RMAN> CONFIGURE DEVICE TYPE 'SBT_TAPE' PARALLELISM 4 BACKUP TYPE TO BACKUPSET;
```

To determine network throughput for a specific time period, use RMAN network analyzer, see MOS note [2022086.1](#)

To diagnose Oracle Cloud Backup Performance, see MOS note [2078576.1](#).

- **Use MULTISECTION backups**

The purpose of multisection backups (available starting Oracle 11g) is to enable RMAN channels to back up a single large file in parallel. RMAN divides the work among multiple channels, with each channel backing up one file section in a file. Backing up a file in separate sections can improve the performance of backups of large data files. For example, suppose that the users tablespace contains a single datafile of 800 MB and assume that four SBT channels are configured, with the parallelism setting for the SBT device set to 4. You can break up the datafile in this tablespace into file sections as shown below.

```
RMAN> BACKUP SECTION SIZE 200M TABLESPACE USERS;
```

*-These procedures will change when the Recovery Appliance is the backup destination.

- **Use “weekly full and daily incremental” strategy**

The goal of an incremental backup is to back up only those data blocks that have changed since a previous backup. This has a lot of benefits but prior to moving toward this standard approach, you should evaluate if your RTO requirements can still be met.

The advantages of this strategy are:

- Reduce the amount of time needed for daily backups. Since backup times are shorter, you have an option to backup more frequently as well to reduce RPO.
- Reduce network usage and network bandwidth requirements when backing up over a network.
- Reduce backup overhead and read I/Os.

The trade off is that restore and recovery time is longer since you have to restore the previous cumulative backup and subsequent incremental plus redo to recover the database.

Below is an example of a Weekly full/daily incremental strategy.

- Sunday
An incremental level 0 backup backs up *all* blocks that have ever been in use in this database.

```
RMAN> BACKUP INCREMENTAL LEVEL 0 DATABASE PLUS ARCHIVELOG NOT BACKED UP DELETE INPUT;
```

- Monday - Saturday
On each day from Monday through Saturday, a differential incremental level 1 backup backs up all blocks that have changed since the most recent incremental backup at level 1 or 0. So, the Monday backup copies blocks changed since Sunday level 0 backup, the Tuesday backup copies blocks changed since the Monday level 1 backup, and so forth.

```
RMAN> BACKUP INCREMENTAL LEVEL 1 DATABASE PLUS ARCHIVELOG NOT BACKED UP DELETE INPUT;
```

RMAN's change tracking feature for incremental backups improves incremental backup performance by recording changed blocks in each datafile in a change tracking file. If change tracking is enabled, RMAN uses the change tracking file to identify changed blocks for incremental backup, thus avoiding the need to scan every block in the datafile.

To enable or disable block change tracking refer to the example below. Additional information can also be found [here](#)

```
SQL>ALTER DATABASE ENABLE BLOCK CHANGE TRACKING;  
SQL>ALTER DATABASE DISABLE BLOCK CHANGE TRACKING;
```

In summary, your RMAN configuration should contain similar settings to the below:

```
CONFIGURE CHANNEL DEVICE TYPE 'SBT_TAPE' PARMS  
'SBT_LIBRARY=/home/oracle/OPC/lib/libopc.so,  
ENV=(OPC_PFILE=/u01/products/db/12.1/dbs/opcodbs.ora)'  
CONFIGURE COMPRESSION ALGORITHM 'MEDIUM'  
CONFIGURE CONTROLFILE AUTOBACKUP ON  
CONFIGURE DEVICE TYPE 'SBT_TAPE' PARALLELISM 4 BACKUP TYPE TO BACKUPSET  
CONFIGURE BACKUP OPTIMIZATION ON
```

You can always list your backups by using the RMAN list command, note the Media attribute name that refers to your storage domain the Oracle Cloud Service.

```

RMAN> LIST BACKUP;
.
.
.
BS Key   Type LV Size          Device Type Elapsed Time Completion Time
-----
48       Full  42.75M   SBT_TAPE    00:01:35    13-SEP-15
        BP Key: 48   Status: AVAILABLE Compressed: YES Tag: TAG20150913T104509
        Handle: 2iqh1tpm_1_1 Media:
myDomain.storage.oraclecloud.com/v1/myService-usoraclei
List of Datafiles in backup set 48
File LV Type Ckp SCN    Ckp Time Name
-----
2       Full  785064   13-SEP-15 /u01/products/oradata/odbslab/sysaux01.dbf
.
.
.

```

Recovery

Because accidents can happen and often without warning, you need to ensure that your backups are available when you need them. Oracle Cloud Backup offers you performance, redundancy, and security, which in turn provide peace of mind. Nevertheless, testing your restore procedures and your backups is still an important activity and should be performed regularly.

Some of the important reasons that require recovery from your backups are below:

1. Storage Failure
2. Block Corruption
3. User/Logical Error
4. Database Failure
5. Site failure or disaster

Pro-actively testing your backups is the key of successful recovery. Below are some important items to consider.

Follow generic Database MAA best practices to detect, prevent and repair from data corruptions.

[Preventing, Detecting, and Repairing Block Corruption - Oracle Database 12c](#)
[Preventing, Detecting, and Repairing Block Corruption: Oracle Database 11g](#)

Crosscheck your backups

Crosschecking your backups is important and it should be done before a delete obsolete. If a backup set, or piece, has gone missing we want to delete it. Crosschecking only marks the missing backup set/piece as expired and does not delete or remove anything. Backup set/pieces marked as expired will not count toward the retention policy of the delete obsolete command.

Following any crosscheck command, it's a good idea to do a corresponding report expired. The delete expired will remove the entries flagged as expired from the RMAN repository.

Use RMAN Crosscheck to check that files are accessible and ready for a restore operation.

```

RMAN> CROSSCHECK BACKUP;
RMAN> CROSSCHECK BACKUP OF DATABASE;
RMAN> LIST EXPIRED BACKUP OF DATABASE;

```

*-These procedures will change when the Recovery Appliance is the backup destination.

Validate your backups

Because media can get corrupted - for several reasons - RMAN provide mechanisms to check for physical and logical corruption for backup residing on a particular media.

RMAN *restore validate* command does a block level check of the backups and ensures that a restore could be performed, by confirming that all database files exist and are free of physical and logical corruptions. It is recommended to validate your backup on a regular basis.

```
RMAN> RESTORE DATABASE VALIDATE CHECK LOGICAL;
```

Note: The RMAN *restore validate* reads the backup sets and check them for corruption. *RMAN restore validate* will consume minimal CPU, memory and network resources to read the backups and analyze them – Restore validate command acts as a normal restore operation but without the overhead of writing any data to storage. The data is streamed from the cloud to your on-premises database for validation purposes and gets discarded after the validation. You may incur in network traffic charges for data leaving the Oracle Cloud (metered service only).

If you have a large backup set, your restore validate command will take longer to complete. For a very quick validation to ensure the backup files are available you can leverage the restore validate in conjunction with the HEADER clause, this will validate if the backups are present but will not validate their content.

***- This is not recommended as the only mean of backup validation.**

```
RMAN>RESTORE DATABASE VALIDATE HEADER;
```

You should also use the backup validate after a backup completion to perform a database validation. The validate command will check for physical corruption in the used blocks only, to extend the check for logical corruptions, you should use check logical in conjunction with the validate command.

```
RMAN>BACKUPVALIDATE CHECK LOGICAL DATABASE ARCHIVELOG ALL;
```

In summary:

- » **Crosscheck:** Ensures that the backup pieces are available on the cloud object store. It will compare the backup metadata (either in the controlfile or catalog) against the physical backup pieces to check if it matches.
- » **Backup validate:** Checks the database datafiles for physical corruptions and with the check logical option, the command checks for logical corruptions as well.
- » **Restore validate:** Checks if the backup is restorable and if it contains any physical corruptions and with the check logical option, the command checks for logical corruptions as well.

Example Plan:

- » Crosscheck daily
- » Restore “check logical” Validate Weekly

*-These procedures will change when the Recovery Appliance is the backup destination.

The calendar below shows a sample backup schedule with validation activities - This is applicable for on premise and Cloud deployments*.

The following validation procedure is recommended:

1. Daily Crosscheck: To ensure that backup pieces are available for restore.
2. Weekly Restore Validate: To confirm that a restore can be performed in the event of a disaster.
3. Bi-Weekly Backup Validate: Executing with check logical will ensure to validate all the used database blocks for physical and logical corruptions.
4. Quarterly Full Restore - To test the DR strategy.

July 16						
Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
June 27	28	29	30	July 1	2	3
<ul style="list-style-type: none"> • Level 1 Backup • Crosscheck • Delete Expired 	<ul style="list-style-type: none"> • Level 1 Backup • Crosscheck • Delete Expired 	<ul style="list-style-type: none"> • Level 1 Backup • Crosscheck • Delete Expired • Restore Validate • Check Logical 	<ul style="list-style-type: none"> • Level 1 Backup • Crosscheck • Delete Expired 	<ul style="list-style-type: none"> • Level 1 Backup • Crosscheck • Delete Expired 	<ul style="list-style-type: none"> • Level 1 Backup • Crosscheck • Delete Expired 	<ul style="list-style-type: none"> • Level 1 Backup • Crosscheck • Delete Expired
4	5	6	7	8	9	10
<ul style="list-style-type: none"> • Level 1 Backup • Crosscheck • Delete Expired 	<ul style="list-style-type: none"> • Level 1 Backup • Crosscheck • Delete Expired 	<ul style="list-style-type: none"> • Level 1 Backup • Crosscheck • Delete Expired • Restore Validate • Check Logical 	<ul style="list-style-type: none"> • Level 1 Backup • Crosscheck • Delete Expired 	<ul style="list-style-type: none"> • Level 1 Backup • Crosscheck • Delete Expired 	<ul style="list-style-type: none"> • Level 1 Backup • Crosscheck • Delete Expired 	<ul style="list-style-type: none"> • Level 1 Backup • Crosscheck • Delete Expired • Backup Database • Check Logical
11	12	13	14	15	16	17
<ul style="list-style-type: none"> • Level 1 Backup • Crosscheck • Delete Expired 	<ul style="list-style-type: none"> • Level 1 Backup • Crosscheck • Delete Expired 	<ul style="list-style-type: none"> • Level 1 Backup • Crosscheck • Delete Expired • Restore Validate • Check Logical 	<ul style="list-style-type: none"> • Level 1 Backup • Crosscheck • Delete Expired 	<ul style="list-style-type: none"> • Level 1 Backup • Crosscheck • Delete Expired 	<ul style="list-style-type: none"> • Level 1 Backup • Crosscheck • Delete Expired 	<ul style="list-style-type: none"> • Level 1 Backup • Crosscheck • Delete Expired
18	19	20	21	22	23	24
<ul style="list-style-type: none"> • Level 1 Backup • Crosscheck • Delete Expired 	<ul style="list-style-type: none"> • Level 1 Backup • Crosscheck • Delete Expired 	<ul style="list-style-type: none"> • Level 1 Backup • Crosscheck • Delete Expired • Restore Validate • Check Logical 	<ul style="list-style-type: none"> • Level 1 Backup • Crosscheck • Delete Expired 	<ul style="list-style-type: none"> • Level 1 Backup • Crosscheck • Delete Expired 	<ul style="list-style-type: none"> • Level 1 Backup • Crosscheck • Delete Expired 	<ul style="list-style-type: none"> • Level 1 Backup • Crosscheck • Delete Expired • Backup Database • Check Logical
25	26	27	28	29	30	31
<ul style="list-style-type: none"> • Level 1 Backup • Crosscheck • Delete Expired 	<ul style="list-style-type: none"> • Level 1 Backup • Crosscheck • Delete Expired 	<ul style="list-style-type: none"> • Level 1 Backup • Crosscheck • Delete Expired • Restore Validate • Check Logical 	<ul style="list-style-type: none"> • Level 1 Backup • Crosscheck • Delete Expired 	<ul style="list-style-type: none"> • Level 1 Backup • Crosscheck • Delete Expired 	<ul style="list-style-type: none"> • Level 1 Backup • Crosscheck • Delete Expired 	<ul style="list-style-type: none"> • Level 1 Backup • Crosscheck • Delete Expired

*-These procedures will change when the Recovery Appliance is the backup destination.



Additional Best Practices:

- » Use RMAN compression (HIGH, MEDIUM, LOW, BASIC) for optimal data transfers.
- » Increase PARALLELISM (until you reach maximum network throughput)
- » Refer to MOS Note 2078576.1 for performance investigation of your backups.
- » If public network throughput is not sufficient, choose Oracle Fast Connect (Standard, Partner Edition, MPLS). Refer to cloud.oracle.com/network
- » Choose cloud storage as appropriate storage tier based on RTO/RPO
- » Perform traditional weekly full and daily incremental backups.
- » You may schedule backing up archived logs frequently to reduce RPO
- » Run Installer once each two months to pick up latest RMAN SBT module
- » Run Installer with new credentials after changing Oracle Cloud password
- » Use Global Namespace to access REST endpoint instead of hard-coding to datacenter specific URLs.
- » Copy `opc<SID>.ora` file to other SIDs if same ORACLE_HOME is used by multiple databases
- » Configure CONTROLFILE AUTOBACKUP ON. This will enable complete restore of a database into a different host.

*-These procedures will change when the Recovery Appliance is the backup destination.



Conclusion

Oracle Cloud Database backup service is an effective and low cost solution to protect your Oracle databases. By leveraging the MAA configuration and operational practices, you have additional guarantees that your restore and recovery operations from Oracle Cloud object store will be successful.







Oracle Corporation, World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065, USA

Worldwide Inquiries
Phone: +1.650.506.7000
Fax: +1.650.506.7200

*-These procedures will change when the Recovery Appliance is the backup destination.



CONNECT WITH US

-  blogs.oracle.com/oracle
-  facebook.com/oracle
-  twitter.com/oracle
-  oracle.com

Integrated Cloud Applications & Platform Services

Copyright © 2016, Oracle and/or its affiliates. All rights reserved. This document is provided *for* information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group. 0615

White Paper Title
April 2017
Author: [OPTIONAL]
Contributing Authors: [OPTIONAL]

*-These procedures will change when the Recovery Appliance is the backup destination.

ÜBER HUNKLER

Das Karlsruher Systemhaus HUNKLER wurde 1988 erster offizieller Partner von Oracle in Deutschland. Ein Team von rund 20 Mitarbeitern unterstützt Kunden aus Industrie, öffentlicher Verwaltung, Gesundheits- und Finanzwesen mit Beratung, Lösungsentwicklung und Managed Services.

Im Fokus von HUNKLER stehen leistungsfähige, wirtschaftliche Infrastrukturen für Oracle-datenbanken mit den Schwerpunkten Hochverfügbarkeit, Ausfallsicherheit und Zero Downtime Migration. Die integrierten Komplettlösungen der Produktfamilie Oracle Engineered Systems sowie der Datenbank-/Anwendungsbetrieb in der Oracle Cloud sind weitere Themenfelder, die das Unternehmen umfassend abdeckt.

HUNKLER
GmbH & Co. KG

Hauptsitz Karlsruhe

Bannwaldallee 32, 76185 Karlsruhe
Tel. 0721-490 16-0, Fax 0721-490 16-29

Geschäftsstelle Bodensee

Fritz-Reichle-Ring 6a
78315 Radolfzell
Tel. 07732-939 14-00, Fax 07732-939 14-04
info@hunkler.de, www.hunkler.de