Ahsay Online Backup Manager v8

Oracle Database Backup and Restore Guide for Linux (GUI)

Ahsay Systems Corporation Limited

11 October 2021

Copyright Notice

Trademarks

Disclaimer

Revision History

Date	Descriptions	Type of modification
25 January 2021	Initial draft	New
18 February 2021	Added examples for Oracle 18c	New
12 March 2021	Added Appendix A	New
7 April 2021	Updated Ch. 7; Added sub-chapters for the detailed process diagrams in Ch. 7.3, 7.4, 7.4.1, 7.4.2 and 7.5	New / Modifications
11 October 2021	Updated login instructions in Ch. 5	Modifications

Table of Contents

1 Overview

1.1 What is this software?

Ahsay brings you specialized client backup software, namely AhsayOBM, to provide a comprehensive backup solution for your Oracle Database Server. The Oracle Database Server module of AhsayOBM provides you with a set of tools to protect your Oracle Server with both full database and archived log backups while your database is online.

1.2 System Architecture

Below is the system architecture diagram illustrating the major elements involved in the backup process among the Oracle Database Server, AhsayOBM and AhsayCBS.

In this user guide, we will focus on the software installation, as well as the end-to-end backup and restore process using AhsayOBM as a client backup software on using Linux GUI mode.
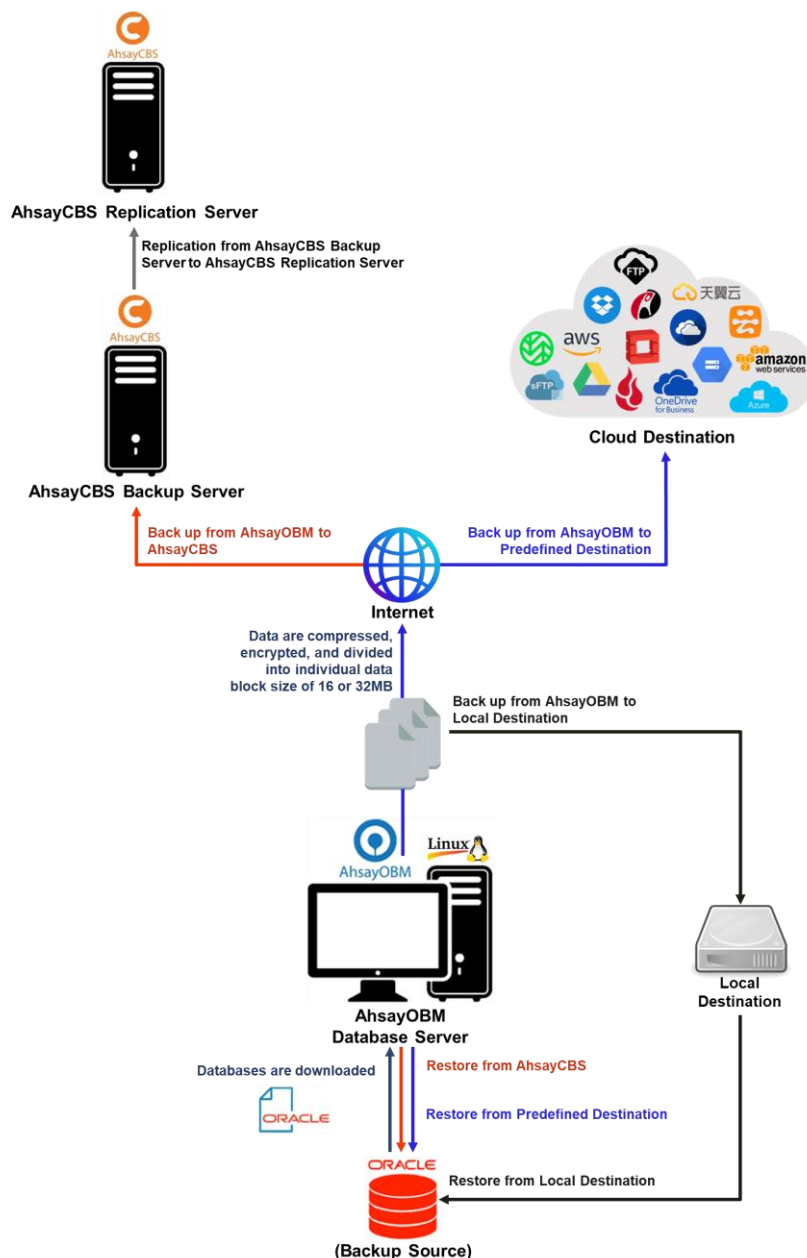
1.3 Oracle Database Backup Mode

Ahsay Oracle database and archived log backups use a spooling method to make a consistent snapshot of the database for backup.

For each database backup job, AhsayOBM will trigger Oracle to spool or make a copy of the following files to the temporary folder:

- Database files (.DBF)
- Archived Log files
- Control files (.CTL)
- Init.ora file
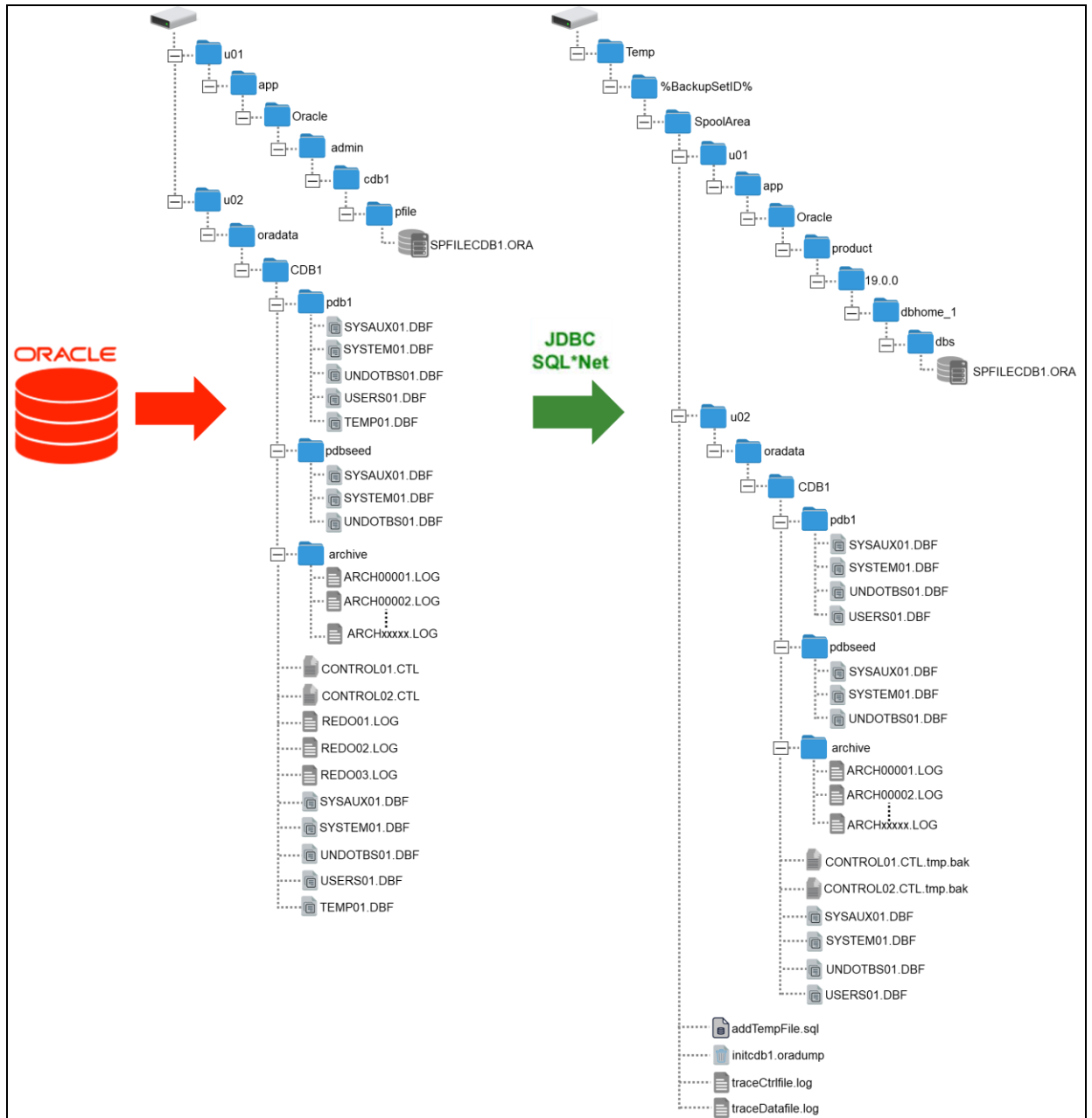
2 Requirements

2.1 Hardware Requirement

Refer to the following article for the list of hardware requirements for AhsayOBM:
FAQ: Ahsay Hardware Requirement List (HRL) for version 8.1 or above

2.2 Software Requirement

Refer to the following article for the list of supported operating systems and application versions:
FAQ: Ahsay Software Compatibility List (SCL) for version 8.1 or above

2.3 AhsayOBM Installation

Make sure the latest version of AhsayOBM is installed directly on the machine where the Oracle database server is hosted.

> **NOTE**
> Backup and restore of Oracle database(s) running on a remote machine is not supported.

2.4 AhsayOBM Add-On Module Configuration

Make sure the Oracle Database Server add-on module is enabled on your AhsayOBM user account.

Please contact your backup service provider for more details.
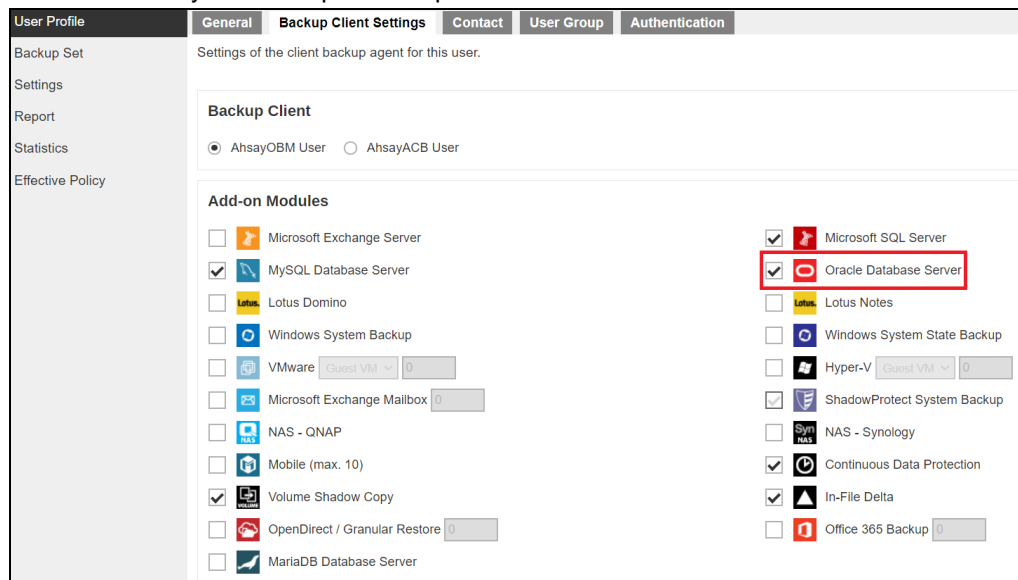
2.5 Backup Quota Requirement

Make sure that your AhsayOBM user account has enough storage quota assigned to accommodate the storage of Oracle database server backup set and retention policy.

2.6 Java Heap Size

The default maximum Java heap size setting on AhsayOBM on Linux is 768MB. For Oracle database backup, it is highly recommended to increase the Java heap size setting to be at least 4096MB to improve backup and restore performance. The actual heap size is dependent on the amount of free memory available on your Oracle server.

For details on how to modify the Java heap size setting of AhsayOBM/AhsayACB, refer to the following article:

2.7 Temporary Directory Folder

The Temporary directory folder is used by AhsayOBM during a backup job as the storage of:

- The spooled Oracle database(s) and archived log files

- Any incremental or differential delta files generated

It is strongly recommended that the temporary directory folder is located on a local drive with enough free disk space to be used by the spooled databases and archived log files. The temporary folder should **not** be located on the Oracle Home drive.

NOTE

The calculation of disk space required on the drive where the temporary folder is located is as follows:

(Total Database Size * Delta Ratio) * number of backup destinations = **Minimum Free Space Required**

Example:

If the default Delta ratio is 50% for in-file delta, and if the total Oracle database size is 1TB and there is only one backup destination, the minimum free space needed on the drive where the temporary directory folder is located = 1.5TB:

1TB = Total Oracle database size

500GB = Total maximum size of incremental or differential delta files generated

To obtain the size of the data files on the Oracle database instance, use the Oracle RMAN REPORT SCHEMA feature and sum up the total "List of Permanent Datafiles" by running the following command.

NOTE: The values shown are just examples and might be different on your Oracle instance.

```
$ export ORACLE_SID=cdb1

$ rman target /

Recovery Manager: Release 19.0.0.0.0 - Production on Fri Nov 6 11:04:21 2020

Version 19.3.0.0.0


Copyright (c) 1982, 2019, Oracle and/or its affiliates.  All rights reserved.


connected to target database: CDB1 (DBID=981637913)


RMAN> report schema;


using target database control file instead of recovery catalog

Report of database schema for database with db_unique_name CDB1



List of Permanent Datafiles
===========================



File  Size(MB) Tablespace        RB segs   Datafile Name

---- -------- -------           -------   -----------------------
```

```
1    920         SYSTEM              YES         /u02/oradata/CDB1/system01.dbf

3    660         SYSAUX              NO          /u02/oradata/CDB1/sysaux01.dbf

4    335         UNDOTBS1            YES         /u02/oradata/CDB1/undotbs01.dbf

5    270         PDB$SEED:SYSTEM     NO          /u02/oradata/CDB1/pdbseed/system01.dbf

6    330         PDB$SEED:SYSAUX     NO          /u02/oradata/CDB1/pdbseed/sysaux01.dbf

7    5           USERS               NO          /u02/oradata/CDB1/users01.dbf

8    100         PDB$SEED:UNDOTBS1   NO          /u02/oradata/CDB1/pdbseed/undotbs01.dbf

9    270         PDB1:SYSTEM         YES         /u02/oradata/CDB1/pdb1/system01.dbf

10   340         PDB1:SYSAUX         NO          /u02/oradata/CDB1/pdb1/sysaux01.dbf

11   100         PDB1:UNDOTBS1       YES         /u02/oradata/CDB1/pdb1/undotbs01.dbf

12   5           PDB1:USERS          NO          /u02/oradata/CDB1/pdb1/users01.dbf


List of Temporary Files
=======================

File Size(MB) Tablespace  Maxsize(MB) Tempfile Name

---- -------- ----------  ----------- --------------------

1    132      TEMP            32767   /u02/oradata/CDB1/temp01.dbf

2    36       PDB$SEED:TEMP 32767     /u02/oradata/CDB1/pdbseed/temp012019-05-10_17-58-06-
785-PM.dbf

3    36       PDB1:TEMP       32767   /u02/oradata/CDB1/pdb1/temp01.dbf
```

2.8 Linux Requirements

Ensure that the following Linux requirements and conditions are met.

2.8.1 Supported OS Version

Oracle 19c (from v8.5.0.63 or above)

The backup of Oracle 19c is supported on the following OS versions:

- Red Had Enterprise Linux 7 and 8 (or above)

Oracle 18c (from v8.5.0.77 or above)

The backup of Oracle 18c is supported on the following OS versions:

- Red Hat Enterprise Linux 6.4 and 7 (or above)

2.8.2 GUI Desktop Environment

The Linux machine must be installed with a GUI desktop environment (i.e., GNOME, KDE, Cinnamon etc.).

2.9 Oracle Backup Requirements

Ensure that the following requirements and conditions on the Oracle database server are met.

NOTE: Please consult your Oracle database administrator before making any changes.

2.9.1 Oracle Tools

Although the following tools are usually installed by default on all Oracle database installations, ensure that the following tools are installed on the Oracle database server, and they are functioning correctly.

- **RMAN (Recovery manager)** - is required by AhsayOBM for both full database and archive log backups.

  To verify if RMAN is installed on the Oracle database server and is working properly, run the following command.

  Example of RMAN running in Oracle 19c

  ```
  $ export ORACLE_SID=cdb1
  $ rman target /

  Recovery Manager: Release 19.0.0.0.0 - Production on Fri
  Nov 6 11:04:21 2020

  Version 19.3.0.0.0

  Copyright (c) 1982, 2019, Oracle and/or its affiliates.
  All rights reserved.

  connected to target database: CDB1 (DBID=981637913)

  RMAN>
  ```

- **SQL*Plus** – is required by AhsayOBM during Oracle Backup Set creation, backup and restore.

  To verify if SQL*Plus is installed on the Oracle database server and is working properly, run the following command `sqlplus / as sysdba`.

  Example of SQL*Plus running in Oracle 19c

  ```
  $ sqlplus / as sysdba

  SQL*Plus: Release 19.0.0.0.0 – Production on Thu Nov 5
  11:32:52 2020

  Version 19.3.0.0.0

  Copyright (c) 1982, 2019, Oracle.  All rights reserved.

  Connected to:

  Oracle Database 19c Enterprise Edition Release 19.0.0.0.0
  – Production

  Version 19.3.0.0.0

  SQL>
  ```

2.9.2 Oracle Internal Process Checking

For the Oracle instance to run smoothly, ensure that the following internal processes are working well:

- **PMON** (Process Monitor)
- **PSP0** (Process Spawner Process)
- **MMAN** (Memory Manager Process)
- **DBW0** (Database Writer)
- **ARC0** (Archive Process)
- **LGWR** (Log Writer)

- **CKPT** (Checkpoint process)
- **SMON** (System Monitor)
- **RECO** (Distributed Recovery Background Process)

To check this, open the Terminal application.

Run the SQLPlus to connect to the Oracle database server. Once connected, use the following SQL query to verify if the internal processes are running.

```
$ sqlplus / as sysdba

SQL*Plus: Release 19.0.0.0.0 - Production on Thu Nov 5 11:32:52
2020

Version 19.3.0.0.0

Copyright (c) 1982, 2019, Oracle.  All rights reserved.

Connected to:

Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 -
Production

Version 19.3.0.0.0


SQL> select name, description from v$bgprocess where PADDR <>
'00';

NAME   DESCRIPTION
-----  ------------------------------------------------------------
PMON   process cleanup
CLMN   process cleanup
PSP0   process spawner 0
VKTM   Virtual Keeper of TiMe process
GEN0   generic0
MMAN   Memory Manager
M004   MMON slave class 1
GEN1   generic1
SCMN
DIAG   diagnosibility process
OFSD   Oracle File Server BG


NAME   DESCRIPTION
-----  ------------------------------------------------------------
SCMN
DBRM   DataBase Resource Manager
VKRM   Virtual sKeduler for Resource Manager
SVCB   services background monitor
PMAN   process manager
DIA0   diagnosibility process 0
DBW0   db writer process 0
LGWR   Redo etc.
CKPT   checkpoint
LG00   Log Writer Slave
```

```
SMON  System Monitor Process

NAME   DESCRIPTION
-----  ------------------------------------------------------------
LG01   Log Writer Slave
SMCO   Space Manager Process
RECO   distributed recovery
W000   space management slave pool
LREG   Listener Registration
W001   space management slave pool
PXMN   PX Monitor
FENC   IOServer fence monitor
MMNL   Manageability Monitor Process 2
MMON   Manageability Monitor Process
D000   Dispatchers

NAME   DESCRIPTION
-----  ------------------------------------------------------------
S000   Shared servers
TMON   Transport Monitor
M000   MMON slave class 1
M002   MMON slave class 1
TT00   Redo Transport
ARC0   Archival Process 0
TT01   Redo Transport
ARC1   Archival Process 1
ARC2   Archival Process 2
ARC3   Archival Process 3
TT02   Redo Transport

NAME   DESCRIPTION
-----  ------------------------------------------------------------
AQPC   AQ Process Coord
W002   space management slave pool
CJQ0   Job Queue Coordinator
P000   Parallel query slave
P001   Parallel query slave
P002   Parallel query slave
P003   Parallel query slave
P004   Parallel query slave
P005   Parallel query slave
P006   Parallel query slave
P007   Parallel query slave

NAME   DESCRIPTION
-----  ------------------------------------------------------------
W003   space management slave pool
M001   MMON slave class 1
W004   space management slave pool
QM02   QMON MS
W005   space management slave pool
W006   space management slave pool
W007   space management slave pool
```

```
Q004   QMON MS
M005   MMON slave class 1
Q005   QMON MS

65 rows selected.


SQL>
```

2.9.3 Supported Oracle Database Server Version

AhsayOBM supports the following version of Oracle database server:

- **Oracle 19c**

- **Oracle 18c**

To verify if the Oracle database server version is supported by AhsayOBM, use the following SQL query.

Oracle 19c

```
$ sqlplus / as sysdba

SQL*Plus: Release 19.0.0.0.0 - Production on Thu Nov 5 11:32:52
2020

Version 19.3.0.0.0

Copyright (c) 1982, 2019, Oracle.   All rights reserved.

Connected to:

Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 -
Production

Version 19.3.0.0.0

SQL>
```

Oracle 18c

```
$ sqlplus / as sysdba

SQL*Plus: Release 18.0.0.0.0 - Production on Mon Jan 4 11:06:36
2021

Version 18.3.0.0.0

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

Connected to:

Oracle Database 18c Enterprise Edition Release 18.0.0.0.0 -
Production

Version 18.3.0.0.0

SQL>
```

2.9.4   System Identifier (SID)

Make sure the System Identifier (SID) is correct by using the following SQL query.

```
SQL> select instance from v$thread;

INSTANCE
-----------------------------------------------------------
cdb1

SQL>
```

NOTE: The instance shown is just an example. The SID may be different on your Oracle instance.

Another way to verify the SID is by checking the **init.ora** file. Go to the **/u01/app/oracle/admin/cdb1/pfile** directory and open the **init.ora** file using a text editor (e.g., vi).

```
###########################################
# Database Identification
###########################################
db_name="cdb1"
```

2.9.5   Oracle_Home Path

Oracle 19c

The Oracle_Home path can be obtained by using the following SQL query. The Oracle_Home path for Oracle 19c is "**/u01/app/oracle/product/19.0.0/dbhome_1**".

```
SQL> SELECT file_spec FROM DBA_LIBRARIES WHERE library_name =
     'DBMS_SUMADV_LIB';

FILE_SPEC
---------------------------------------------------------
/u01/app/oracle/product/19.0.0/dbhome_1/lib/libqsmashr.so

SQL>
```

NOTE: The directory path shown is just an example. The Oracle_Home path may be different on your Oracle instance.

Another way to verify the Oracle_Home path is by checking the **init.ora** file. Go to the **/u01/app/oracle/admin/cdb1/pfile** directory and open the **init.ora** file using a text editor (e.g., vi).

```
###########################################
# File Configuration
###########################################
control_files=("/u01/app/oracle/oradata/CDB1/control01.ctl", "/u01/app/oracle
oradata/cdb1/control02.ctl")
###########################################
```

Oracle 18c

The Oracle_Home path can be obtained by using the following SQL query. The Oracle_Home path for Oracle 18c is "**/u01/app/oracle/product/18.0.0/dbhome_1**".

```
SQL> SELECT file_spec FROM DBA_LIBRARIES WHERE library_name =
     'DBMS_SUMADV_LIB';


FILE_SPEC
------------------------------------------------------------
/u01/app/oracle/product/18.0.0/dbhome_1/lib/libqsmashr.so


SQL>
```

NOTE: The directory path shown is just an example. The Oracle_Home path may be different on your Oracle instance.

Another way to verify the Oracle_Home path is by checking the **init.ora** file. Go to the **/u01/app/oracle/admin/cdb1/pfile** directory and open the **init.ora** file using a text editor (e.g., vi).

WARNING: The value of the Oracle_Home path in init.ora file needs to match the value obtained from the SQL query. If the value does not match, please contact the Oracle database administrator for further assistance.

2.9.6 Database Status

Ensure that the status of Oracle instance is "Open". To check, use the following query.

```
SQL> select instance_name, status from v$instance;


INSTANCE_NAME    STATUS
-------------    ---------------------------------------------
cdb1             OPEN


SQL>
```

2.9.7 Archived Log Mode

Ensure that the database instance is in Archived Log mode. To check, use the following command.

```
SQL> archive log list;


Database log mode              Archive Mode
Automatic archival             Enabled
Archive destination /u01/app/oracle/product/19.0.0/dbhome_1/dbs/arch
Oldest online log sequence     42
Next log sequence to archive   44
Current log sequence           44


SQL>
```

NOTE: The values shown are just examples and might be different on your Oracle instance.

2.9.8   Java Installation

Java must be installed on the Oracle Database. To check if Java is installed, use the following SQL query. The status of the **JServer JAVA Virtual Machine** and **Oracle Database Java Packages** should be "VALID".

```
SQL> select comp_name, status from dba_registry;

COMP_NAME                               STATUS
-------------                           ------------

Oracle Database Catalog Views           VALID

Oracle Database Packages and Types      VALID

Oracle Real Application Clusters        OPTION OFF


COMP_NAME                               STATUS
-------------                           ------------

JServer JAVA Virtual Machine            VALID

Oracle XDK                              VALID

Oracle Database Java Packages           VALID


COMP_NAME                               STATUS
-------------                           ------------

OLAP Analytic Workspace                 VALID

Oracle XML Database                     VALID

Oracle Workspace Manager                VALID


COMP_NAME                               STATUS
-------------                           ------------

Oracle Text                             VALID

Oracle Multimedia                       VALID

Spatial                                 VALID


COMP_NAME                               STATUS
-------------                           ------------

Oracle OLAP API                         VALID

Oracle Label Security                   VALID
```

```
Oracle Database Vault                              VALID

15 rows selected.

SQL>
```

2.9.9 JAVASYSPRIV Permission for Oracle System Account

The Oracle **system** account is used by AhsayOBM to connect to the Oracle database server to authenticate the backup and restore process. The following permission must be assigned to the system account. Use the following SQL query to assign.

```
SQL> select * from DBA_ROLE_PRIVS where
upper(grantee)='SYSTEM';

GRANTEE        GRANTED_ROLE              ADM DEL DEF COM INH
-------        ----------                --- --- --- --- ---
SYSTEM         JAVASYSPRIV               NO   YES NO

SYSTEM         DBA                       NO   YES NO


GRANTEE        GRANTED_ROLE              ADM DEL DEF COM INH
-------        ----------                --- --- --- --- ---
SYSTEM         AQ_ADMINISTRATOR_ROLE     YES  NO  YES  NO

SQL>
```

If not, grant javasyspriv to the system account by using the following SQL query.

```
SQL> grant javasyspriv to system;

Grant succeeded.

SQL>
```

2.9.10 SYSDBA Privileges for Oracle System Account

To check if the system account has **sysdba** privileges, use the following SQL query.

```
SQL> select * from v$pwfile_users where sysdba='TRUE';

USERNAME SYSDB SYSOP SYSAS SYSBA SYSDG SYSKM ACCOUNT_STATUS
-------- ----- ----- ----- ----- ----- ----- --------------
SYSTEM   TRUE  FALSE FALSE OPEN

SQL>
```

If not, grant **sysdba** to the system account using the following SQL query.

Oracle 19c and Oracle 18c

```
SQL> grant sysdba to system container=ALL;

Grant succeeded.

SQL>
```

2.9.11 TNS Listener Service

TNS listener service must be started to allow connections to the Oracle database server. To check if the TNS listener service is running, use the *lsnrctl status* command.

If the TNS listener service is not started, use the *lsnrctl start* command to start the service.

Example: A running TNS Listener service on Oracle 19c.

```
$ lsnrctl status

LSNRCTL for Linux: Version 19.0.0.0.0 - Production on 05-NOV-
  2020 11:33:44

Copyright (c) 1991, 2019, Oracle.  All rights reserved.

Connecting to
  (DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=oracle19c.local)(POR
  T=1521)))
STATUS of the LISTENER
-----------------------
Alias                     LISTENER
Version                   TNSLSNR for Linux: Version 19.0.0.0.0
  - Production
Start Date                03-NOV-2020 12:13:24
Uptime                    1 days 23 hr. 20 min. 20 sec
Trace Level               off
Security                  ON: Local OS Authentication
SNMP                      OFF
Listener Parameter File
  /u01/app/oracle/product/19.0.0/dbhome_1/network/admin/listener
  .ora
Listener Log File
  /u01/app/oracle/diag/tnslsnr/oracle19c/listener/alert/log.xml
Listening Endpoints Summary...

  (DESCRIPTION=(ADDRESS=(PROTOCOL=tcp)(HOST=oracle19c.local)(POR
  T=1521)))
  (DESCRIPTION=(ADDRESS=(PROTOCOL=ipc)(KEY=EXTPROC1521)))
Services Summary...
Service "86b637b62fdf7a65e053f706e80a27ca" has 1 instance(s).
  Instance "cdb1", status READY, has 1 handler(s) for this
  service...
Service "8886b84fb1e0709de053631e100a76ed" has 1 instance(s).
  Instance "cdb1", status READY, has 1 handler(s) for this
  service...
Service "cdb1" has 1 instance(s).
  Instance "cdb1", status READY, has 1 handler(s) for this
  service...
Service "cdb1XDB" has 1 instance(s).
  Instance "cdb1", status READY, has 1 handler(s) for this
  service...
Service "pdb1" has 1 instance(s).
```

```
   Instance "cdb1", status READY, has 1 handler(s) for this
 service...
The command completed successfully
```

NOTE: The values shown are just examples and might be different on your Oracle instance.

2.9.12 Localhost is Resolvable

Verify if the localhost IP 127.0.0.1 on the Oracle database server is resolvable using the **ping** command as this will be the IP address that AhsayOBM will use to connect to the Oracle instance.

```
# ping -c4 127.0.0.1

PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.

64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.043 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.043 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.032 ms
64 bytes from 127.0.0.1: icmp_seq=4 ttl=64 time=0.038 ms

--- 127.0.0.1 ping statistics ---

4 packets transmitted, 4 received, 0% packet loss, time 2999ms

rtt min/avg/max/mdev = 0.032/0.039/0.043/0.004 ms
```

2.9.13 Oracle Port Number

The default Oracle port number is **1521**. To check, use the **netstat** and **tnsping** commands to verify the actual port number.

NETSTAT

```
# netstat -pan|more
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address   Foreign Address   State        PID/Program name
tcp   0      0      0.0.0.0:111      0.0.0.0:*         LISTEN       1/systemd
tcp   0      0      192.168.122.1:53 0.0.0.0:*         LISTEN       6054/dnsmasq
tcp   0      0      0.0.0.0:22       0.0.0.0:*         LISTEN       5218/sshd
tcp   0      0      127.0.0.1:631    0.0.0.0:*         LISTEN       5220/cupsd
tcp   0      0      127.0.0.1:25     0.0.0.0:*         LISTEN       5513/master
tcp   0      0      10.16.30.99:49829 10.16.30.99:1521 ESTABLISHED 6523/ora_lreg_cdb1
tcp6  0      0      :::31181         :::*              LISTEN       6535/ora_d000_cdb1
tcp6  0      0      :::111           :::*              LISTEN       1/systemd
tcp6  0      0      :::50000         :::*              LISTEN       7140/bschJW
tcp6  0      0      :::1521          :::*              LISTEN       6965/tnslsnr
tcp6  0      0      :::22            :::*              LISTEN       5218/sshd
tcp6  0      0      ::1:631          :::*              LISTEN       5220/cupsd
tcp6 0       0      127.0.0.1:60024  :::*              LISTEN       7140/bschJW
tcp6 0       0      ::1:25           :::*              LISTEN       5513/master
tcp6 0       0      10.16.30.99:1521 10.16.30.99:49829 ESTABLISHED 6965/tnslsnr
```

NOTE: The values shown are just examples and might be different on your Oracle instance.

TNSPING

```
$ tnsping 127.0.0.1

TNS Ping Utility for Linux: Version 19.0.0.0.0 - Production on
06-NOV-2020 10:18:56
```

```
Copyright (c) 1997, 2019, Oracle.  All rights reserved.

Used parameter files:
/u01/app/oracle/product/19.0.0/dbhome_1/network/admin/sqlnet.or
a

Used EZCONNECT adapter to resolve the alias
Attempting to contact
(DESCRIPTION=(CONNECT_DATA=(SERVICE_NAME=))(ADDRESS=(PROTOCOL=t
cp)(HOST=127.0.0.1)(PORT=1521)))
OK (0 msec)
```

3 Best Practices and Recommendations

1. To enable a full Oracle database instance recovery, all databases including **SYSAUX**, **SYSTEM**, **UNDOTBS1**, **USERS** and related application databases except for "TEMP" must be selected in the backup source when creating the backup set. Otherwise, without a backup of these databases, a full Oracle database instance recovery will NOT be possible.

2. Full database backup or incremental / differential database backups should be scheduled when system activity is low to achieve the best possible performance and to minimize the impact on the database server performance (for example: scheduled to run on weekends).

3. For **Archived Log backups**, the backup frequency should be dependent on the number of transactions or activity on the database. Databases with more transaction should run archived log backup more frequently (for example: instead of a daily backup, it should be run multiple times a day).

4. To provide **maximum data protection** and **flexible restore options**, it is recommended to configure:

   - At least one offsite or cloud destination
   - At least one local destination for fast recovery

5. Perform **test restores** periodically to ensure that your backup is set up and data are backed up properly.

   Performing recovery tests can also help identify potential issues or gaps in your recovery plan. It is important that you do not try to make the test easier, as the objective of a successful test is not to demonstrate that everything is flawless. There might be flaws identified in the plan throughout the test and it is important to identify those flaws.

6. The **Restore Raw File** option is for advanced Oracle database administrators and should only be used if you have in-depth knowledge and understanding of Oracle database engine, Oracle database schema, knowledge of the database server and network infrastructure. Therefore, it is not recommended to use this restore option as there is need to utilize additional Oracle techniques and scripts to facilitate a manual database restore.

   Please refer to the following article of Oracle Database Backup and Recovery User's Guide for details:

   Oracle 19c
   https://docs.oracle.com/en/database/oracle/oracle-database/19/bradv/index.html

   Oracle 18c
   https://docs.oracle.com/en/database/oracle/oracle-database/18/bradv/index.html

7. To ensure an optimal backup/restoration performance, it is highly recommended to set the temporary directory folder to a local disk location with sufficient free disk space. It must **not** be on the location of the Oracle Home drive.

4 Limitations

1. For Oracle database server on Linux CLI environment, AhsayOBM does not fully support all restore options. Whenever possible, it is strongly recommended to use Linux GUI for restore.

2. AhsayOBM does not support Oracle Express Edition or Oracle XE.

3. Backup and restore of Oracle database(s) running on a remote machine is not supported.

4. AhsayOBM Oracle database module only supports backup and/or restore of standalone Oracle installations. The following advanced Oracle database setups are not supported:

   - Clusterware or RAC (Real Application Clusters)
   - ASM (Automatic Storage Management)
   - Data Guard etc.

5. An AhsayOBM Oracle database backup set supports the backup and restore of one Oracle instance. For Oracle database server's setup with multiple instances, a separate backup set is required for each instance.

6. To recover a full Oracle database instance, the following items must be selected in the backup source:

   - Oracle Database Server must be selected.
   - All databases including **SYSAUX**, **SYSTEM**, **UNDOTBS1**, **USERS** and related application databases except for "TEMP" must be selected in the backup source when creating the backup set. Otherwise, without a backup of these databases, a full Oracle database instance recovery will NOT be possible.
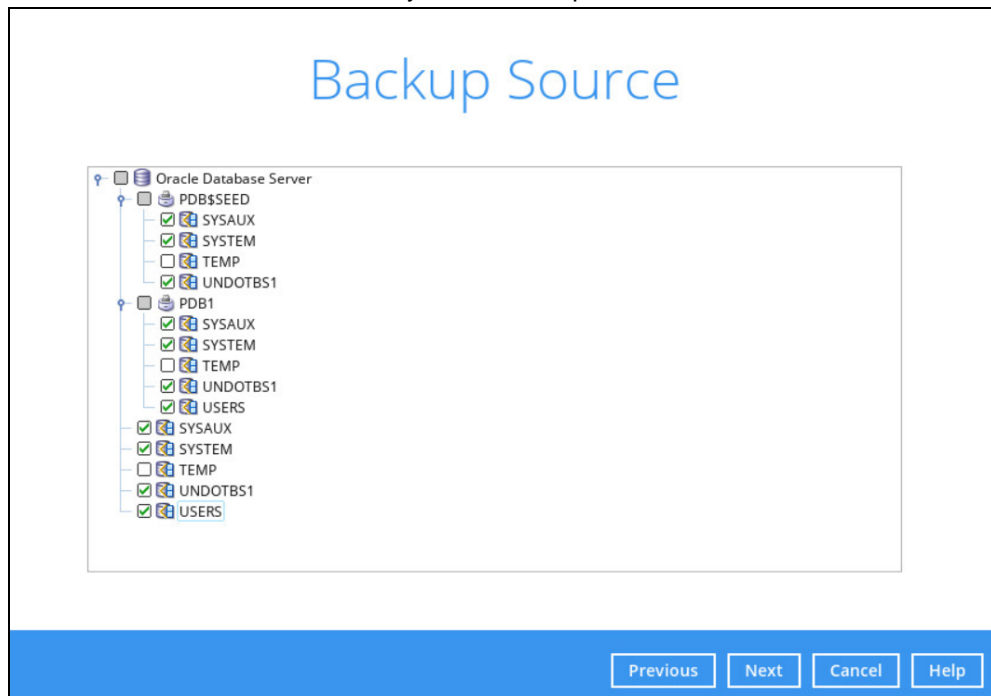
NOTE: Even if the "TEMP" is selected in the backup source, this database will be skipped during a backup job.

5 Logging in to AhsayOBM

Starting with AhsayOBM v8.5.0.0, there are several login scenarios depending on the setting of the account you are using. The different scenarios will be discussed below:

- Login without 2FA

- Login with 2FA using authenticator app

- Login with 2FA using Twilio

5.1 Login to AhsayOBM without 2FA

1. On the Linux GUI, go to **Applications > Other** then click the AhsayOBM to launch the application.
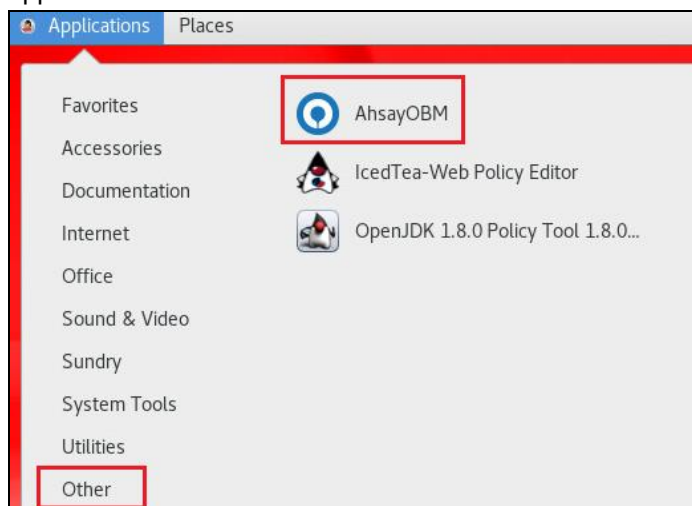
2. Enter the **Login name** and **Password** of your AhsayOBM account, then click **OK** to log in.
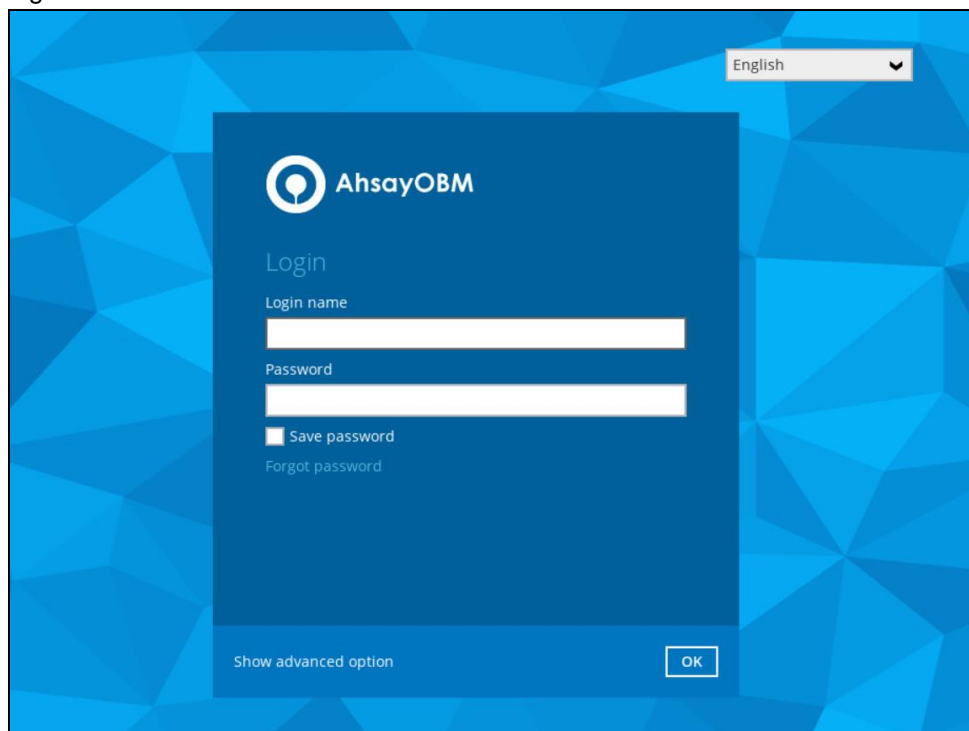
3. After successful login, the following screen will appear.
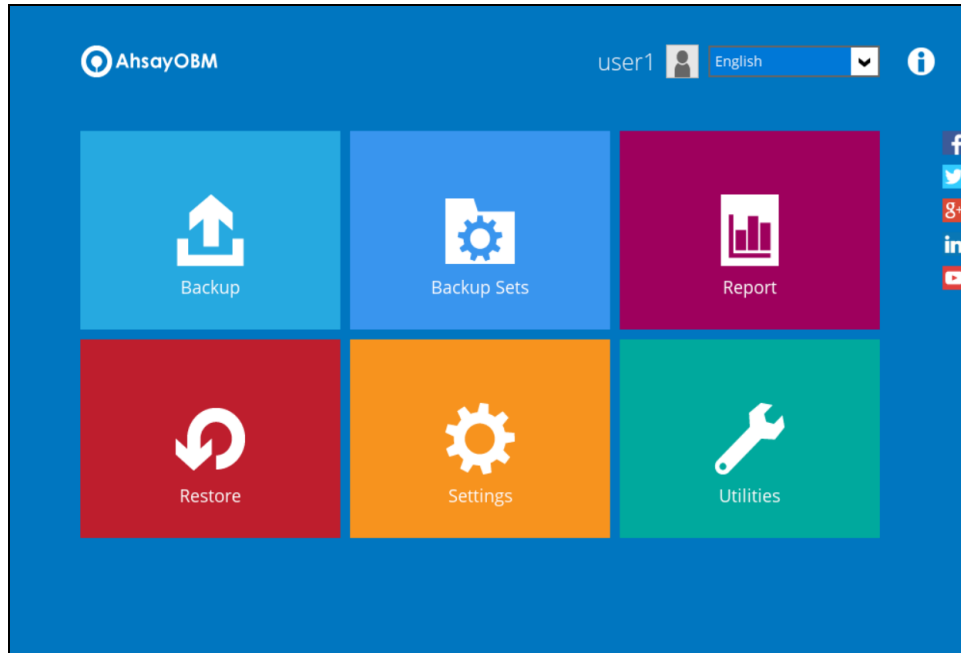
5.2 Login to AhsayOBM with 2FA using authenticator app

1. On the Linux GUI, go to **Applications > Other** then click the AhsayOBM to launch the application.
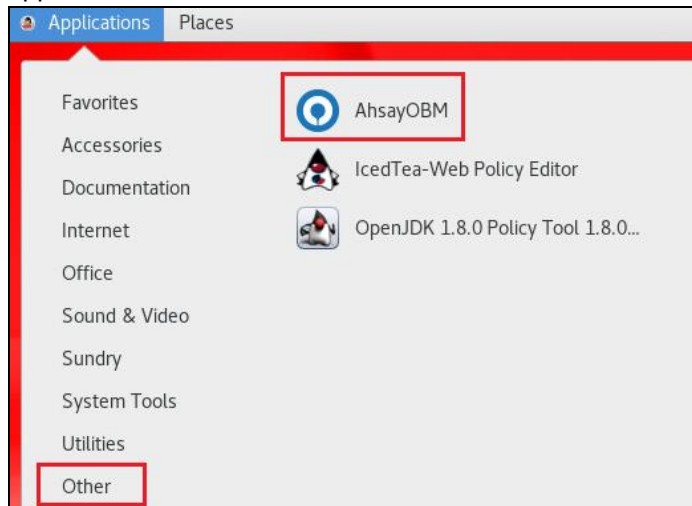
2. Enter the **Login name** and **Password** of your AhsayOBM account, then click **OK** to log in.
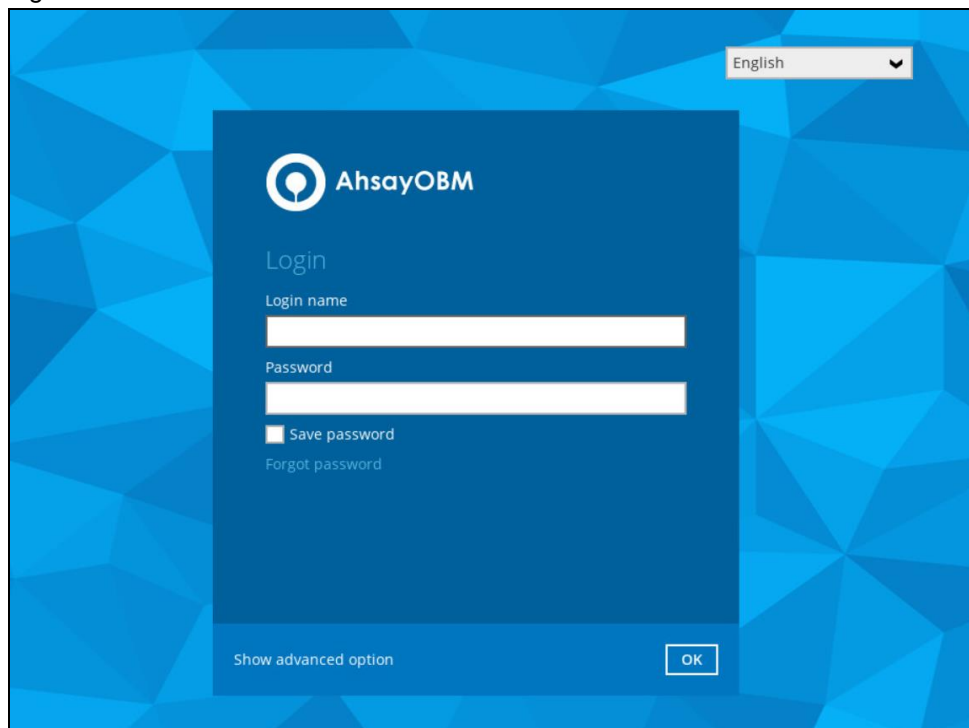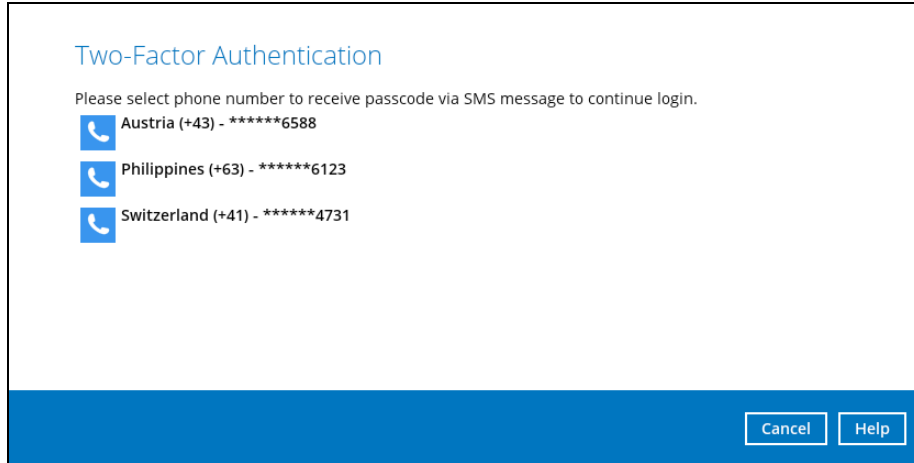

3. One of the two authentication methods will be displayed to continue with the login:

- Push Notification and TOTP when using Ahsay Mobile app

- TOTP only

  ➢ If **Ahsay Mobile app** was configured to use Push Notification and TOTP, then there are two 2FA modes that can be used:

    • Push Notification (default)

      Push notification is the default 2FA mode. Accept the login request on Ahsay Mobile to complete the login.
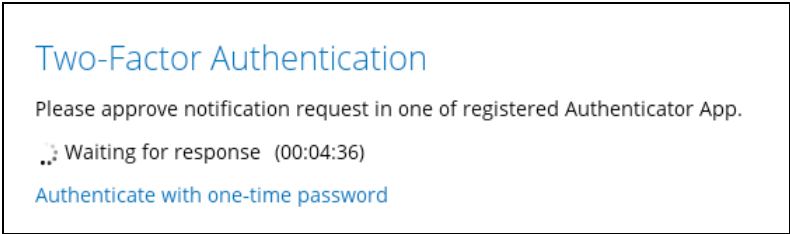
Example of the login request sent to the Ahsay Mobile app.
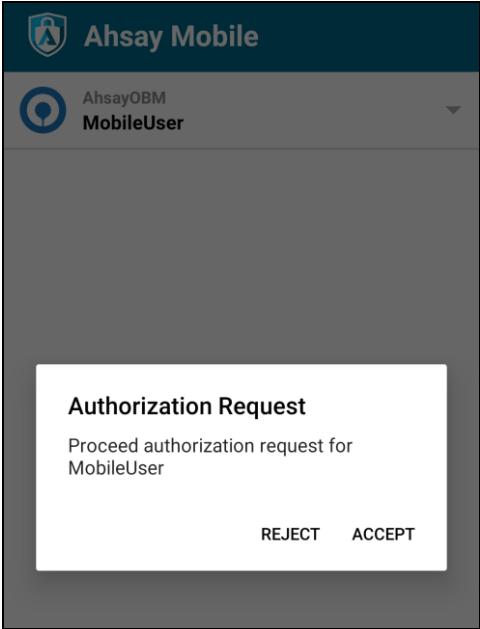
- TOTP

However, if push notification is not working or you prefer to use one-time passcode, click the Authenticate with one-time password link, then input the one-time passcode generated by Ahsay Mobile to complete the login.
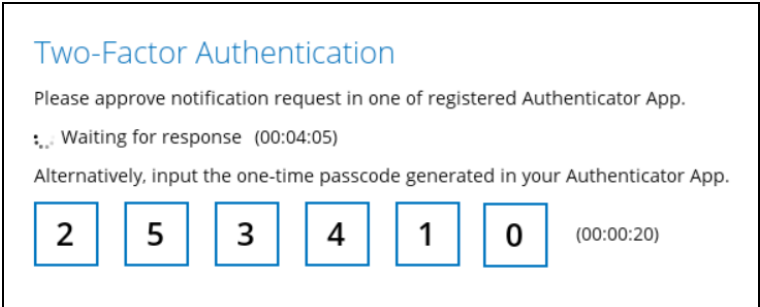
Example of the one-time passcode generated in the Ahsay Mobile app.
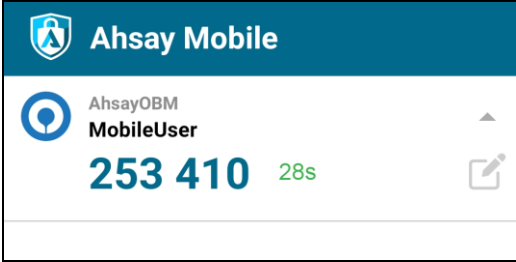
➢ TOTP only

Enter the one-time passcode generated by the authenticator app to complete the login.
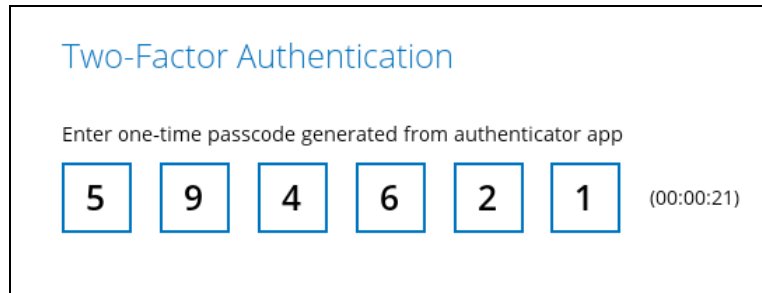
Example of the one-time passcode generated in the third-party authenticator app Microsoft Authenticator.
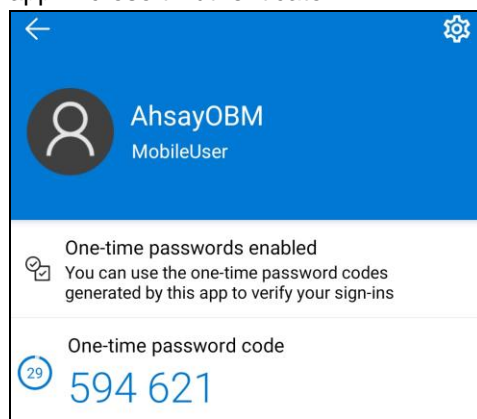
4. After successful login, the following screen will appear.
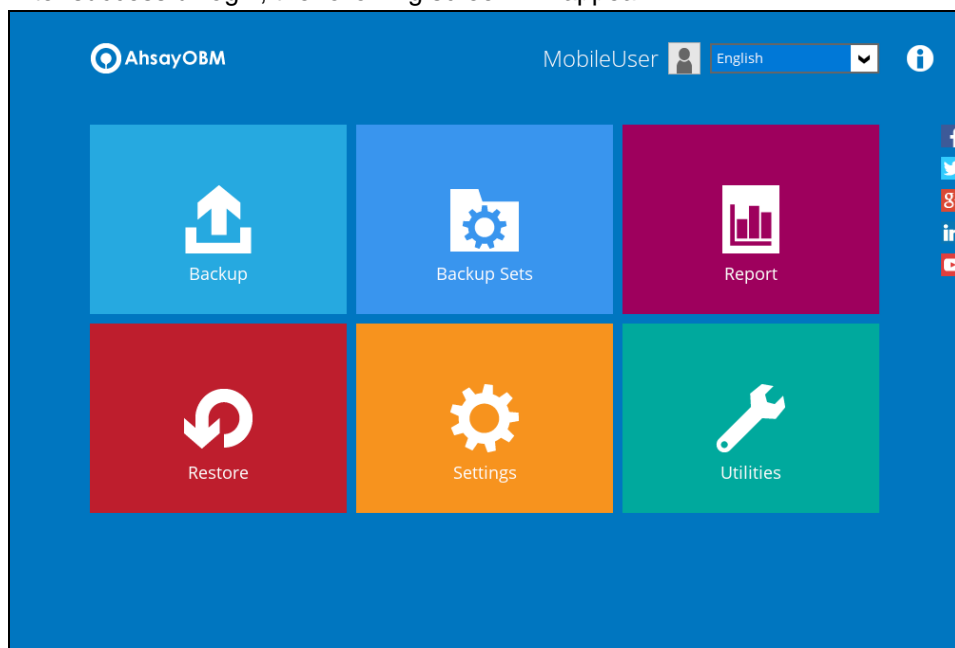
NOTE
If you have trouble logging in using the authenticator app, please refer to Chapter 8 of the AhsayOBM Quick Start Guide for Linux (GUI) for more information.

5.3 Login to AhsayOBM with 2FA using Twilio

1. On the Linux GUI, go to **Applications > Other** then click the AhsayOBM to launch the application.
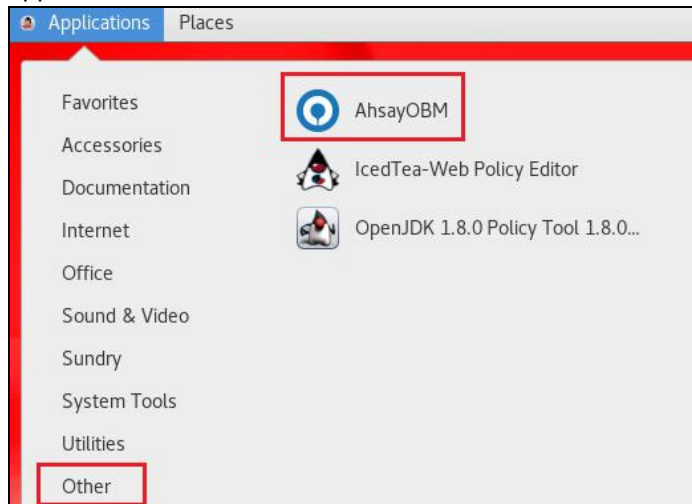
2. Enter the **Login name** and **Password** of your AhsayOBM account, then click **OK** to log in.
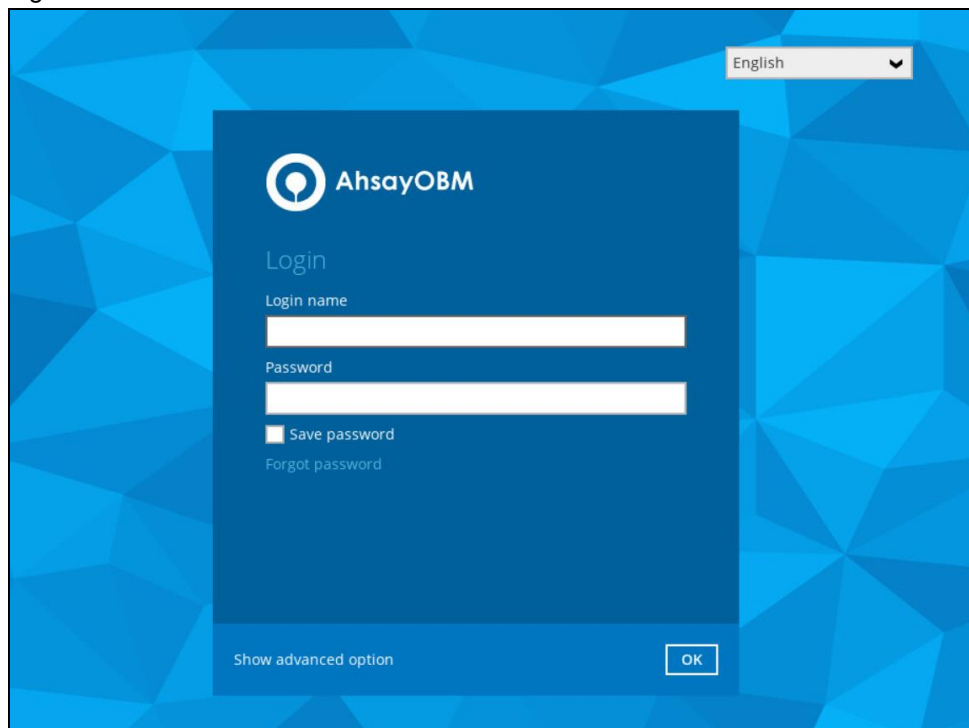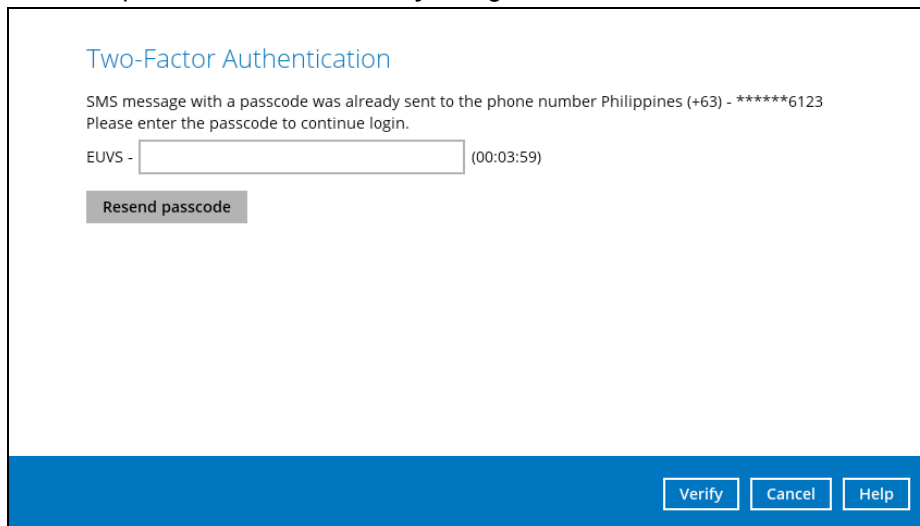
3. Select your phone number.

4. Enter the passcode and click **Verify** to login.
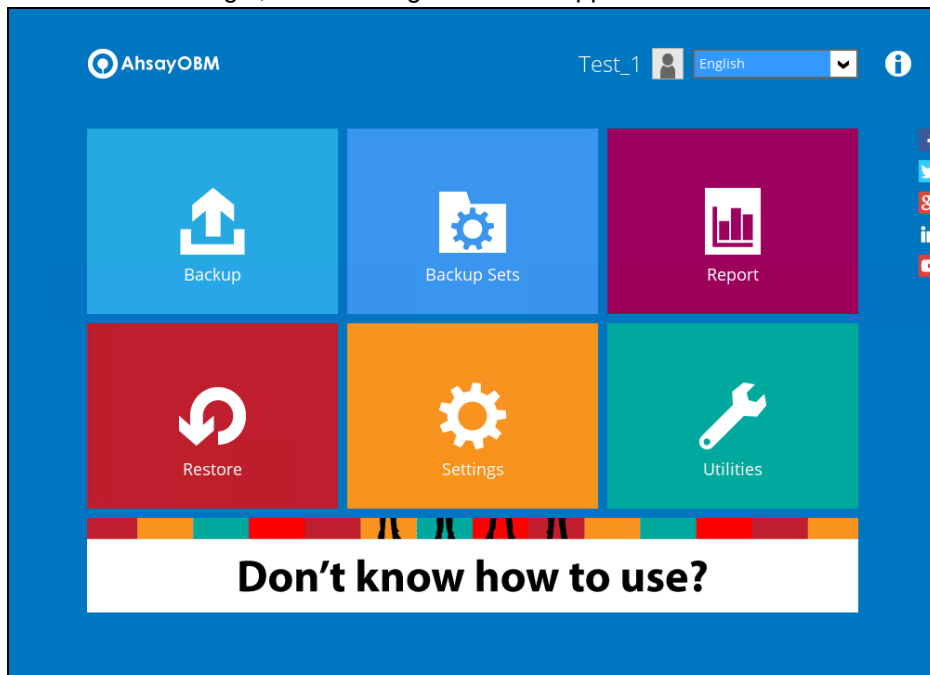
5. After successful login, the following screen will appear.
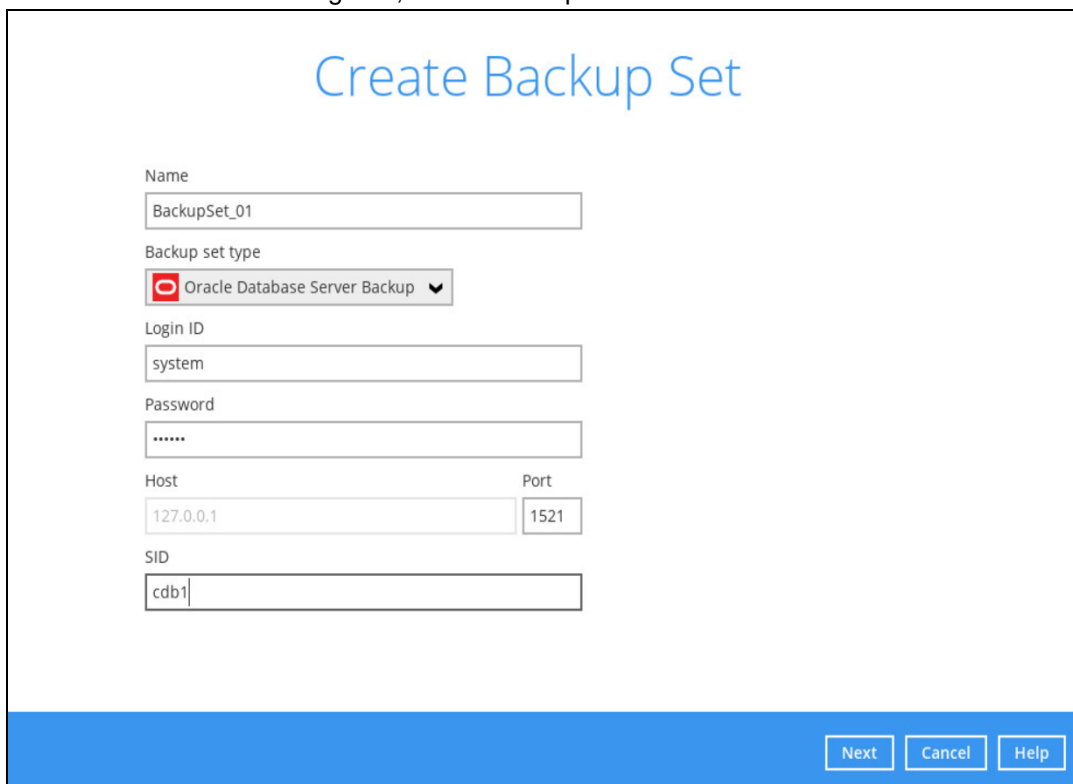
6 Creating an Oracle Database Backup Set

1. Click the Backup Sets icon on the AhsayOBM main interface.

2. Create a new backup set by clicking the **Add** button.

3. In the Create Backup Set window, select Oracle Database Server Backup as the Backup set type. Configure the following settings:

   - **Name** - the name of the backup set.

   - **Backup set type** – the type of the backup set (i.e. Oracle Database Server Backup).

   - **Login ID** – the login ID of the Oracle server. The default login ID is "*system*".

   - **Password** – the password of the login account.

   - **Host** – this value is not user configurable.

   - **Port** – the port where the connections to the Oracle server is made. The default port is "*1521*".

   - **SID** – the Oracle System Identifier. For more details, please refer to Ch. 2.9.4.

   Once all the fields are configured, click **Next** to proceed.

4.   In the Backup Source menu, select the Oracle database(s) you would like to back up. Click **Next** to proceed.
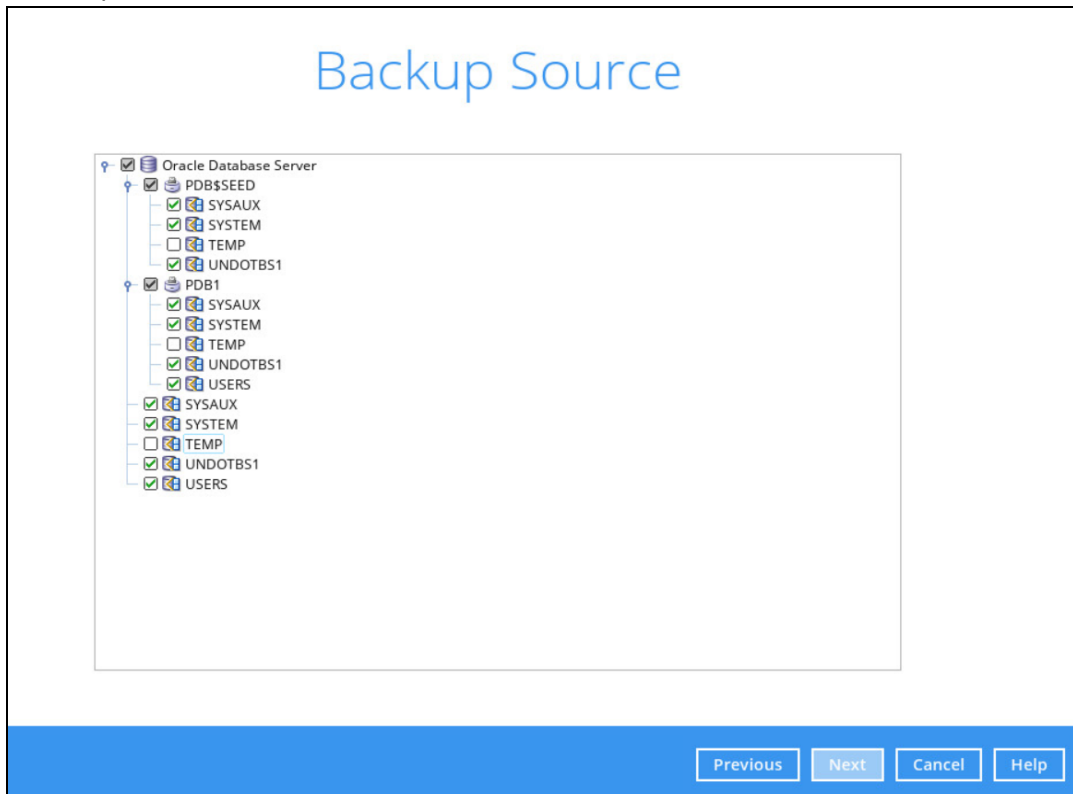
NOTE: All databases including **SYSAUX**, **SYSTEM**, **UNDOTBS1**, **USERS** and related application databases except for "TEMP" must be selected in the backup source when creating the backup set. Otherwise, without a backup of these databases, a full Oracle database instance recovery will NOT be possible.

Even if the "TEMP" is selected in the backup source, this database will be skipped during a backup job.

5. A backup schedule for a backup job to run automatically at your specified time interval can be configured. The backup schedule is enabled by default.
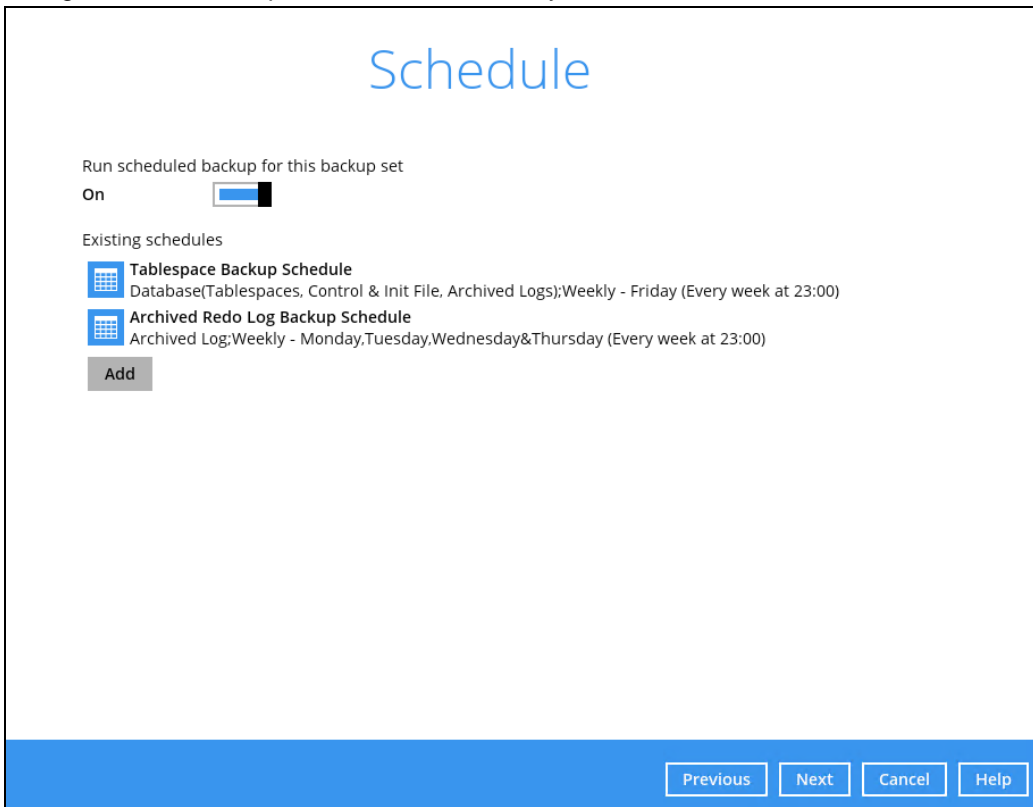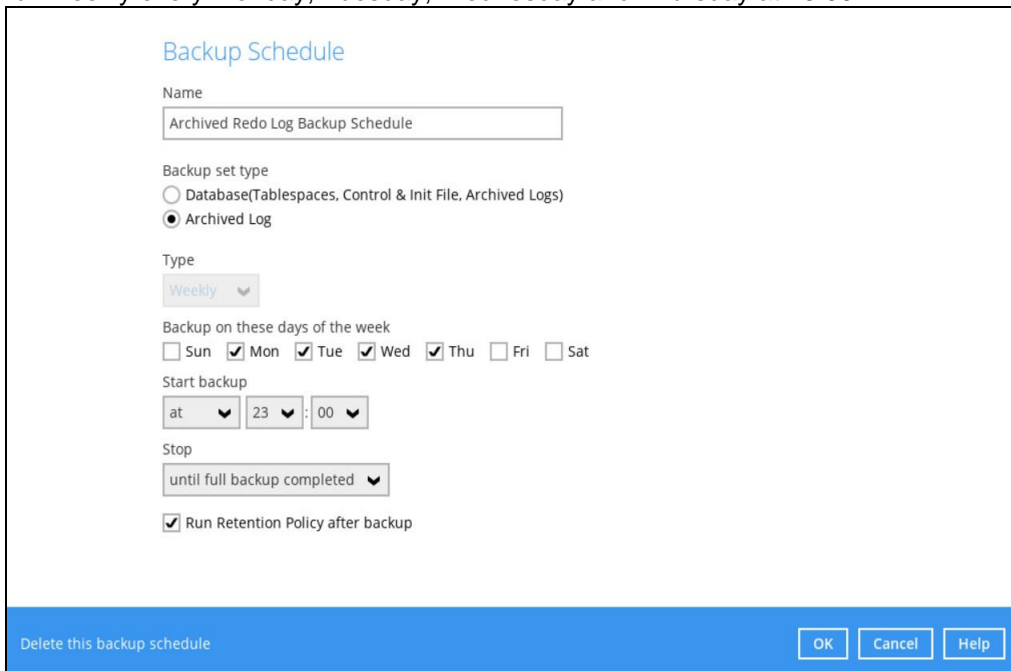
There are two types of backup schedule:

- **Tablespace Backup Schedule**

- **Archived Redo Log Backup Schedule**

Tablespace Backup Schedule – This type of backup scheduler will automatically run weekly every Friday at 23:00.
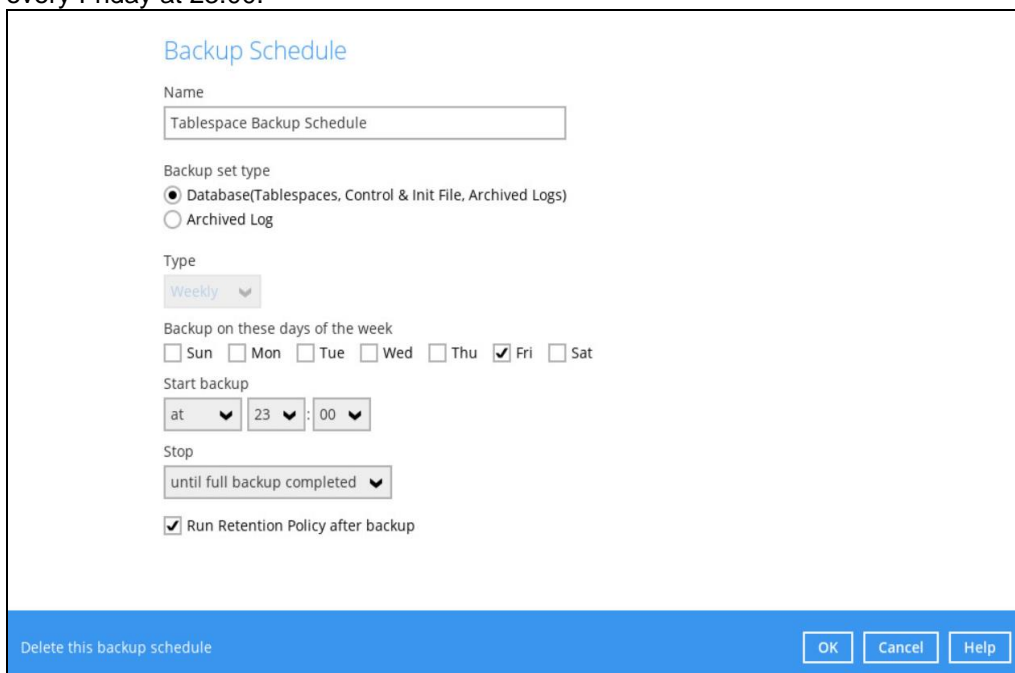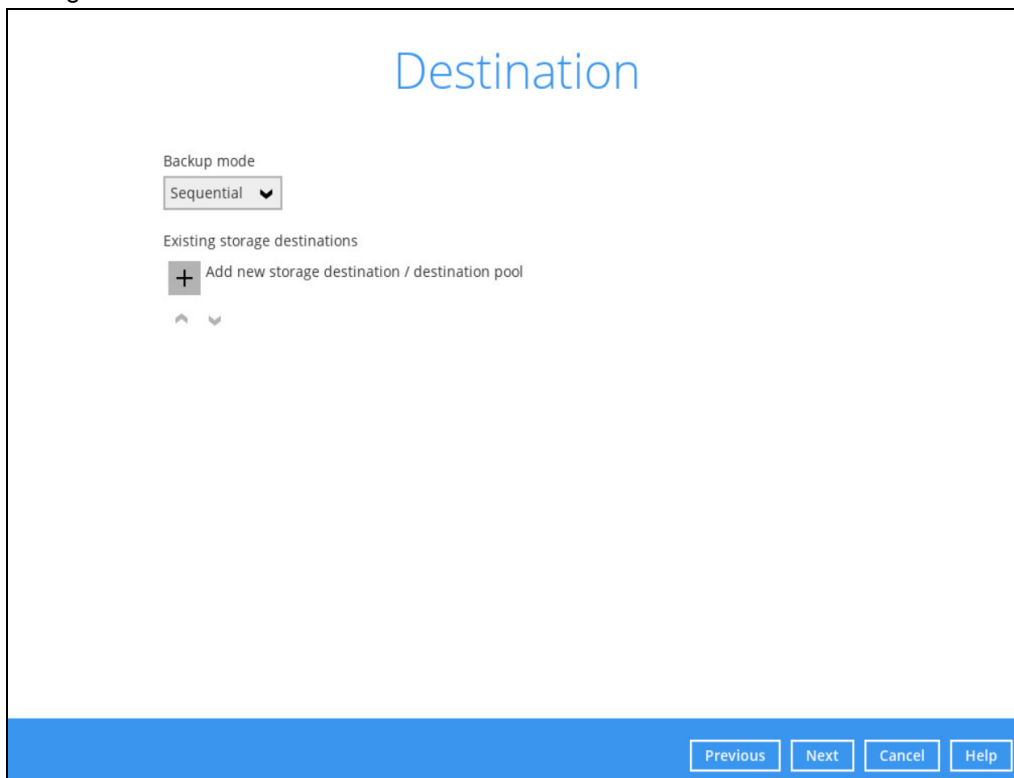
Archived Redo Log Backup Schedule – This type of backup scheduler will automatically run weekly every Monday, Tuesday, Wednesday and Thursday at 23:00.

To change the backup schedule settings of an existing schedule, double-click the schedule to be modified. Otherwise, click **Next** to proceed.

6. In the **Destination** window, select a backup mode then click the + button to add a backup storage destination.

In the **New Storage Destination / Destination Pool** window, select the destination storage. Then, click **OK** to confirm your selection.

If **Local / Mapped Drive / Removable Drive** is selected, specify the path by clicking the **Change** button. After selecting a destination, click the **Test** button check the connection.
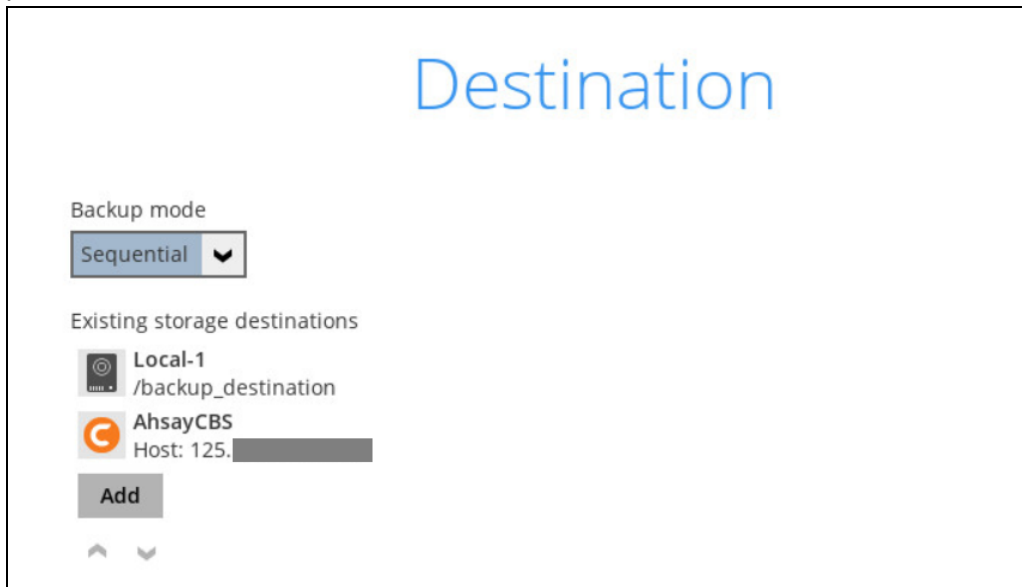
When the **Test completed successfully** message is shown, click **OK** to proceed.

7. In the **Destination** window, your selected storage destination will be shown. Click **Next** to proceed.
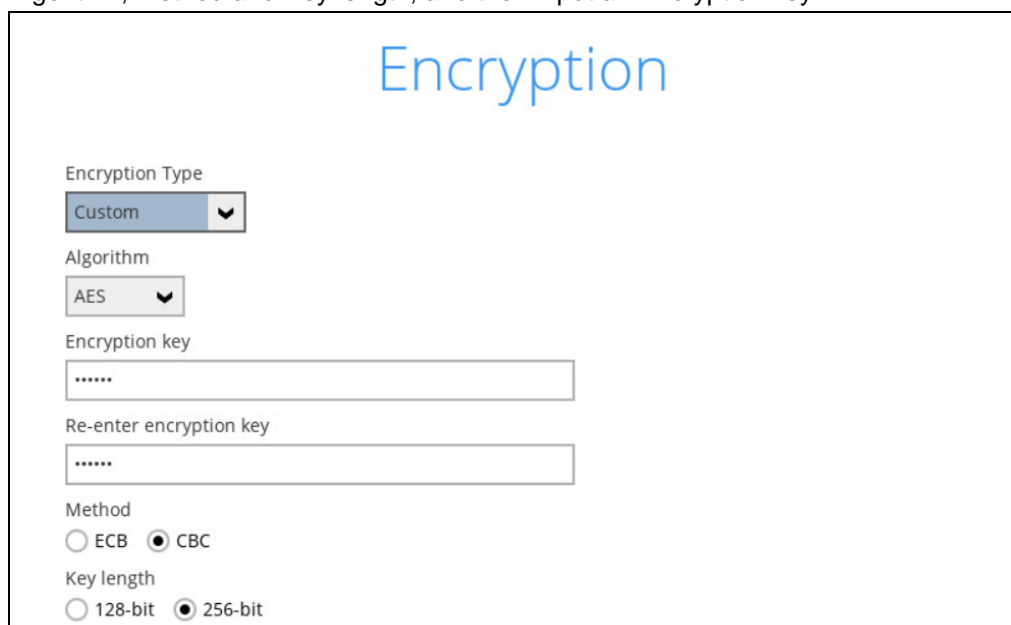
8. In the Encryption window, the **Encrypt Backup Data** option is enabled by default with an encryption key preset by the system.

There are three (3) types of Encryption to choose from:

- **Default** – an encryption key with forty-four (44) alpha numeric characters will be randomly generated by the system.

- **User password** – the encryption key will be the same as the login password of your AhsayOBM at the time when this backup set is created. Please be reminded that if you change the AhsayOBM login password later, the encryption keys of the backup sets previously created with this encryption type **will remain unchanged**.

- **Custom** – the encryption key can be customized where the user can select the Algorithm, Method and Key length, and then input an Encryption key.

Click **Next** once done with the Encryption settings.

9. If the Encryption feature is enabled in the previous step, the following window will pop-up whichever encryption type is selected.
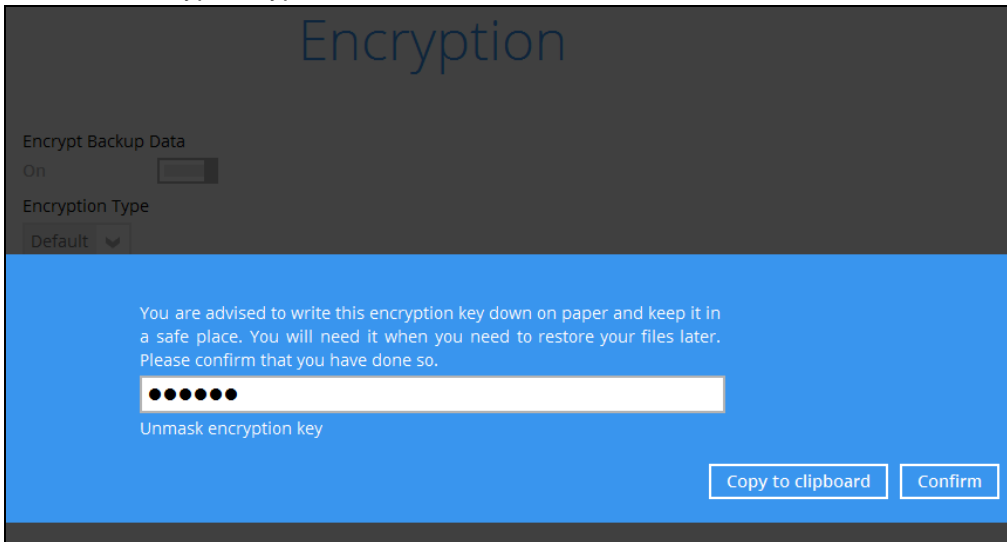
This pop-up window has three (3) options to choose from:

- **Unmask encryption key** – The encryption key is masked by default. Click this option to display the encryption key.
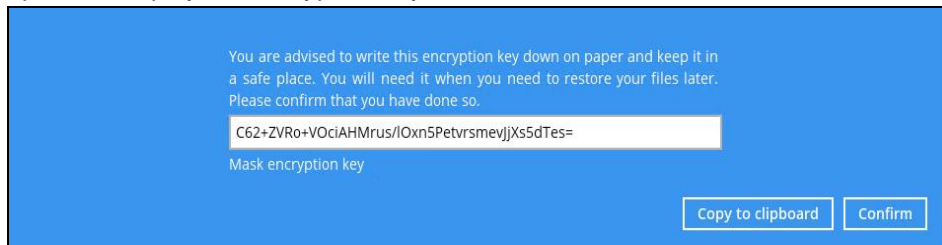
- **Copy to clipboard** – Select this option to copy the encryption key. Once copied, you can paste it to a text editor (e.g., gedit) and save to a location.

- **Confirm** – Select this option to exit the pop-up window and proceed to the next step.

10. After completing all the configuration settings, the Oracle database server backup set will be created.

Congratulations!

"BackupSet_01" is successfully created.

Backup now   Close
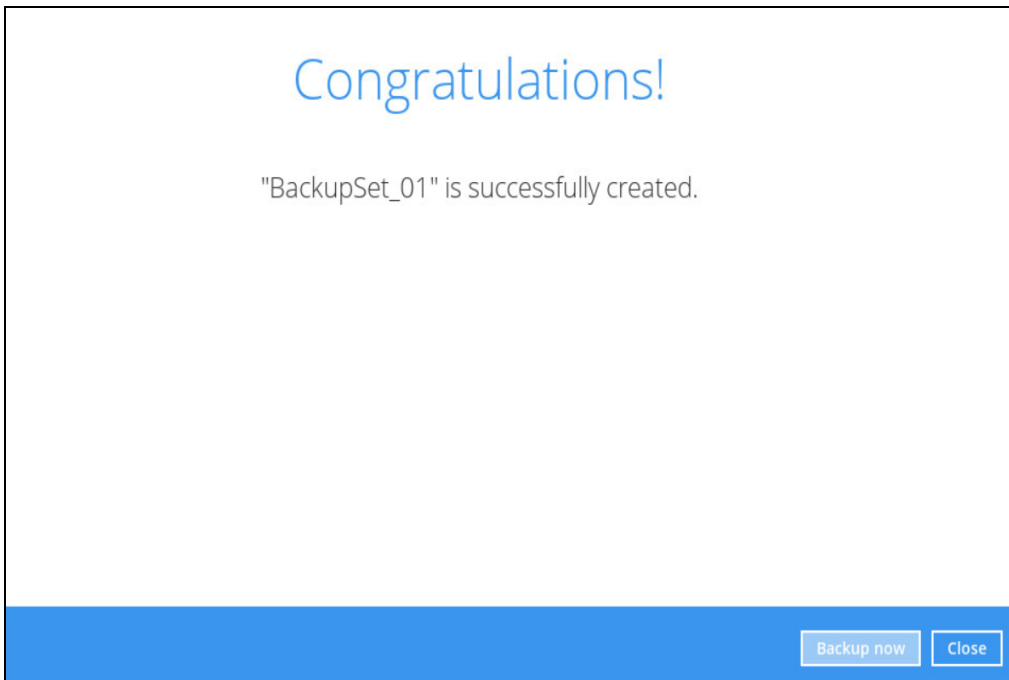
11. According to Best Practices and Recommendations, it is highly recommended to set the temporary directory folder to a local disk location with sufficient free disk space. It must **not** be on the location of the Oracle Home drive. To do this, click the **Backup Sets** icon on the AhsayOBM main interface, then select a backup set. Click **Show advanced settings** link. Go to Others > Temporary Directory and click the **Change** button to browse for another location.

BackupSet_01

General

Source

Backup Schedule

Destination

In-File Delta

Retention Policy

Command Line Tool

Bandwidth Control

Others

Hide advanced settings

Temporary Directory

Temporary directory for storing backup files

/temp   Change

15.99GB free out of total 26.01GB space in /temp
☑ Remove temporary files after backup

Archived Log Deletion

Delete the archived logs after backup
On ▮▮▮

Delete archived logs that are older than the following days

60 ▾ days

Compressions

Select compression type

Fast with optimization for local   ▾

Encryption

Encryption key   ●●●●●●
Copy to clipboard   Unmask encryption key
Algorithm   AES

Delete this backup set   Save   Cancel   Help

Tick the "Remove temporary files after backup" option.

12. Optional: **Archived Log Deletion**

The deletion of the archived logs is enabled by default and archived logs more than 60 days are deleted from the Oracle database instance. This process is done after every databases and archived log backup job.

For example, if the Oracle database instance generates a lot of archived log files, you may want to reduce the number of days before they are deleted.
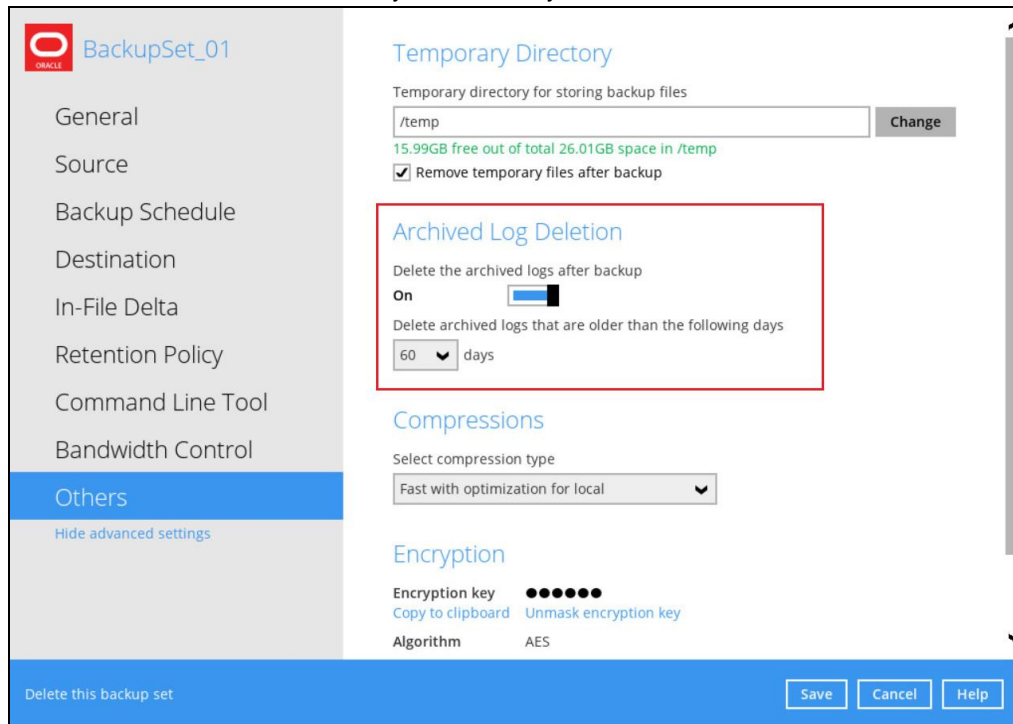
13. Optional: Select your preferred **Compression** type. The compression type is set to **Fast with optimization for local** by default. To change the compression type, go to Others > Compressions.
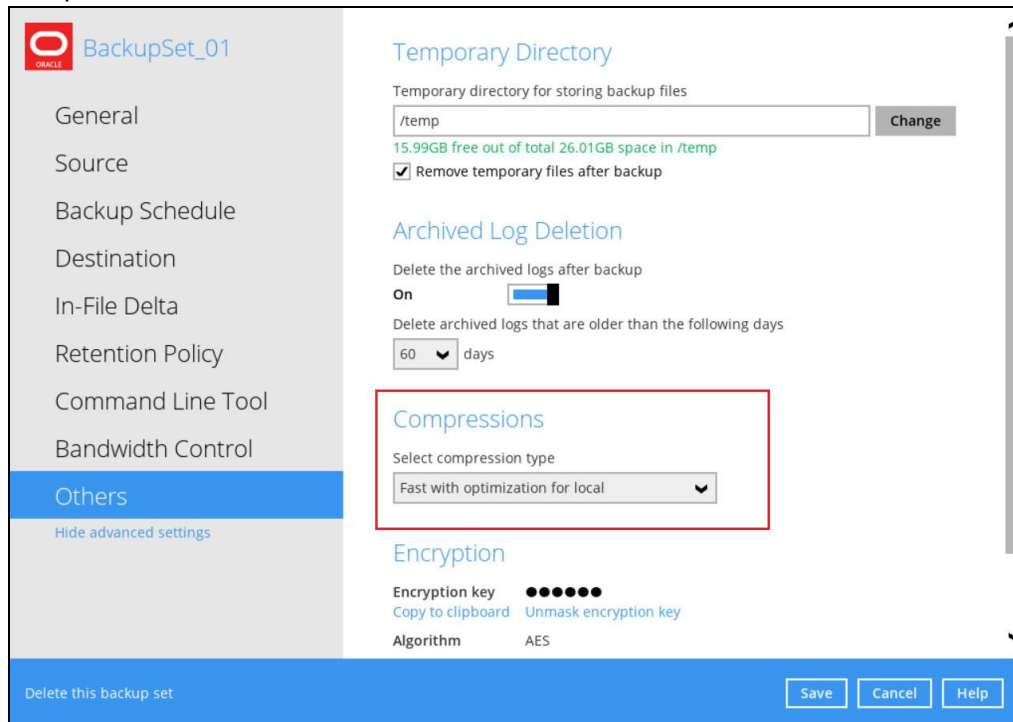
Select from the following:

- No Compression

- Normal

- Fast (Compressed size larger than normal)

- Fast with optimization for local
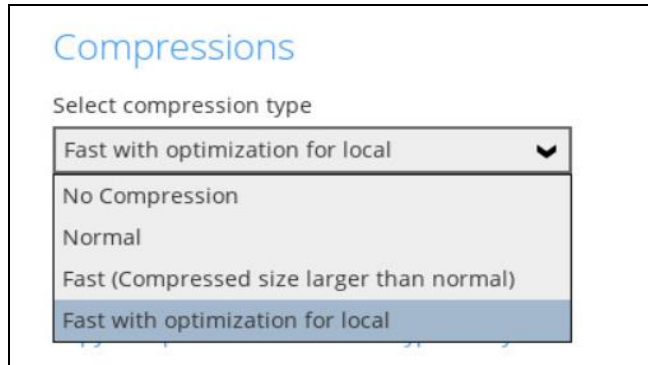
14. Click **Save** to apply the changes.

7 Overview on the Backup Process

The following steps are performed during an Oracle Server backup job in Database and Archived Log backup modes.

7.1 Database Backup

For an overview of the detailed process for Steps **3**, **5**, **11**, and **14**, please refer to the following chapters.

- Periodic Data Integrity Check (PDIC) Process **(Step 3)**
- Backup Set Index Handling Process
  - Start Backup Job **(Step 5)**
  - Completed Backup Job **(Step 14)**
- Data Validation Check Process **(Step 11)**

Start backup job

Step		Description
Establishing connection	1	Connection from the backup client to the backup server is established.
Uploading encryption key	2	Encryption key is uploaded to the backup server (if enabled).
Running Periodic DIC	3	Physical .bak files (data blocks) that do not exist in the index are removed from the backup destination(s), then the statistics of both data area and retention area will be recalculated.
Running pre-backup command	4	Pre-backup command is running (if configured).
Downloading files	5	Latest index.db file and checksum files are downloaded from the backup destination(s) to the temporary folder.
Compiling file list	6	Local file list is compiled according to the backup source setting.
Spooling Oracle databases	7	AhsayOBM issues request to spool database files (.DBF), archived log files, control files (.CTL) and init.ora file from the Oracle server to the temporary folder.
Comparing files	8	Local and remote file lists are compared to identify new, updated, moved, or deleted files and/or folders since the last backup job.
Generating delta files	9	In-file delta files are generated for Oracle Databases (if required when in-file delta is enabled).
Uploading files	10	Data are compressed, encrypted, divided into individual data block size of 16 or 32 MB, and then uploaded to the backup destination(s).
Data validation check	11	The number of 16 or 32 MB data blocks, and the individual block size in the backup destination(s) is identical to the blocks transferred.
Running retention policy	12	Retention policy job is running (if enabled).
Removing archived log files	13	Recovery Manager (RMAN) will remove archived log files from Oracle which are older than xx day(s).
Saving files	14	Latest index files on the client computer are saved to the backup destination(s), and client log files are saved to the backup server.
Running post-backup command	15	Post-backup command is running (if configured).
Removing temporary files	16	Temporary data is removed from the storage location specified in the backup set (if enabled).

Backup job completed

7.2 Archived Log Backup

For an overview of the detailed process for Steps **3**, **5**, **11**, and **14**, please refer to the following chapters.

- Periodic Data Integrity Check (PDIC) Process **(Step 3)**

- Backup Set Index Handling Process

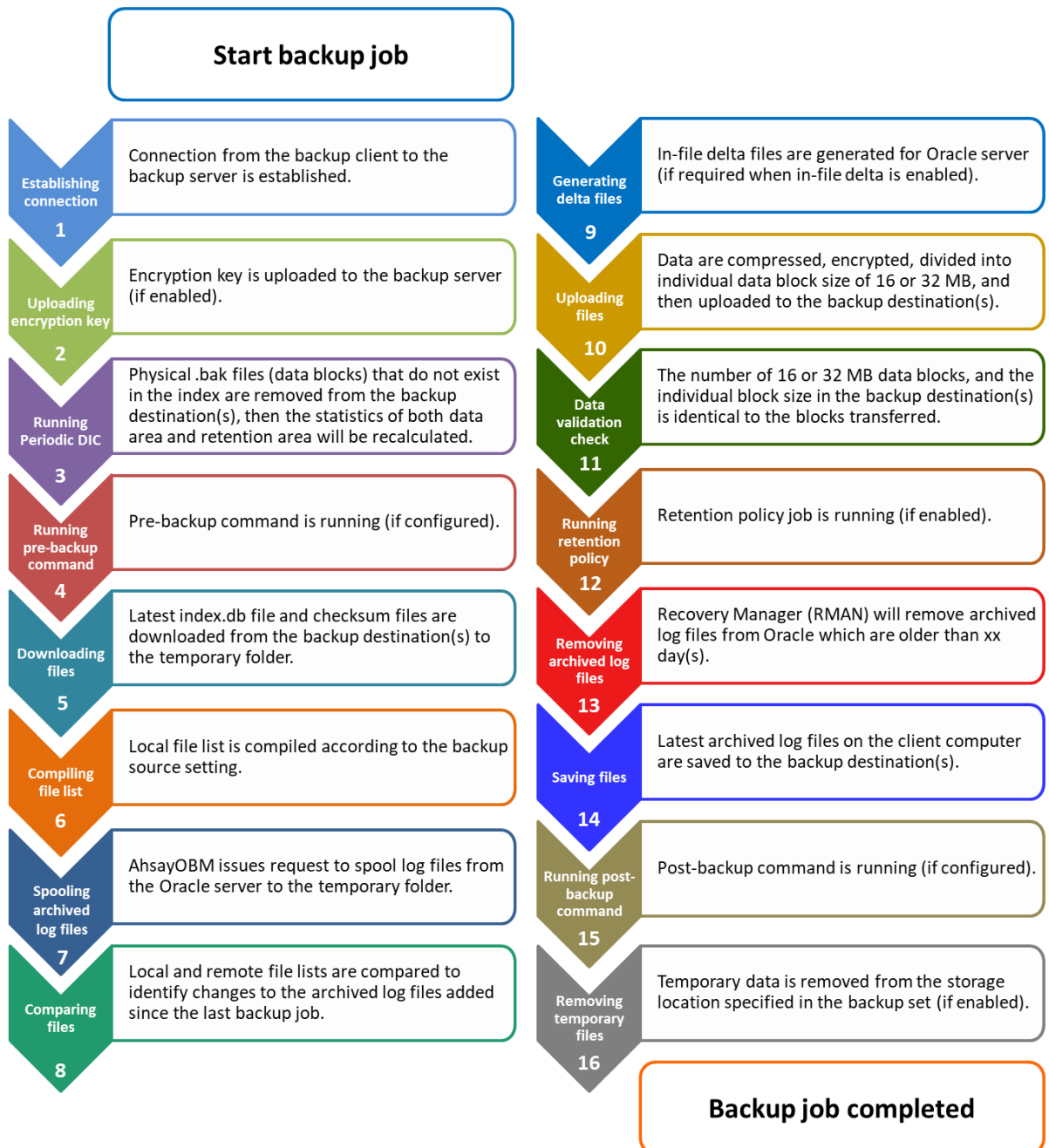 - Start Backup Job **(Step 5)**

  - Completed Backup Job **(Step 14)**

- Data Validation Check Process **(Step 11)**

Start backup job

Establishing connection 1	Connection from the backup client to the backup server is established.
Uploading encryption key 2	Encryption key is uploaded to the backup server (if enabled).
Running Periodic DIC 3	Physical .bak files (data blocks) that do not exist in the index are removed from the backup destination(s), then the statistics of both data area and retention area will be recalculated.
Running pre-backup command 4	Pre-backup command is running (if configured).
Downloading files 5	Latest index.db file and checksum files are downloaded from the backup destination(s) to the temporary folder.
Compiling file list 6	Local file list is compiled according to the backup source setting.
Spooling archived log files 7	AhsayOBM issues request to spool log files from the Oracle server to the temporary folder.
Comparing files 8	Local and remote file lists are compared to identify changes to the archived log files added since the last backup job.

Generating delta files 9	In-file delta files are generated for Oracle server (if required when in-file delta is enabled).
Uploading files 10	Data are compressed, encrypted, divided into individual data block size of 16 or 32 MB, and then uploaded to the backup destination(s).
Data validation check 11	The number of 16 or 32 MB data blocks, and the individual block size in the backup destination(s) is identical to the blocks transferred.
Running retention policy 12	Retention policy job is running (if enabled).
Removing archived log files 13	Recovery Manager (RMAN) will remove archived log files from Oracle which are older than xx day(s).
Saving files 14	Latest archived log files on the client computer are saved to the backup destination(s).
Running post-backup command 15	Post-backup command is running (if configured).
Removing temporary files 16	Temporary data is removed from the storage location specified in the backup set (if enabled).

Backup job completed

7.3 Periodic Data Integrity Check (PDIC) Process

For AhsayOBM v8.3.6.0 (or above), the PDIC will run on the first backup job that falls on the corresponding day of the week from **Monday to Friday**.

To minimize the impact of the potential load of large number of PDIC jobs running at the same time on the AhsayCBS server, the schedule of a PDIC job for each backup set is automatically determined by the result of the following formula:

> **PDIC schedule = %BackupSetID% modulo 5**
> or
> **%BackupSetID% mod 5**

The calculated **result** will map to the corresponding day of the week (i.e., from Monday to Friday).

0	Monday
1	Tuesday
2	Wednesday
3	Thursday
4	Friday

NOTE: The PDIC schedule cannot be changed.

Example:

Backup set ID: 1594627447932

*Calculation: 1594627447932 mod 5 = **2***

2	Wednesday

In this example:

- the PDIC will run on the first backup job that falls on Wednesday; or
- if there is no active backup job(s) running from Monday to Friday, then the PDIC will run on the next available backup job.

NOTE

Although according to the PDIC formula for determining the schedule is **%BackupSetID% mod 5**, this schedule only applies if the previous PDIC job was actually run more than 7 days prior.

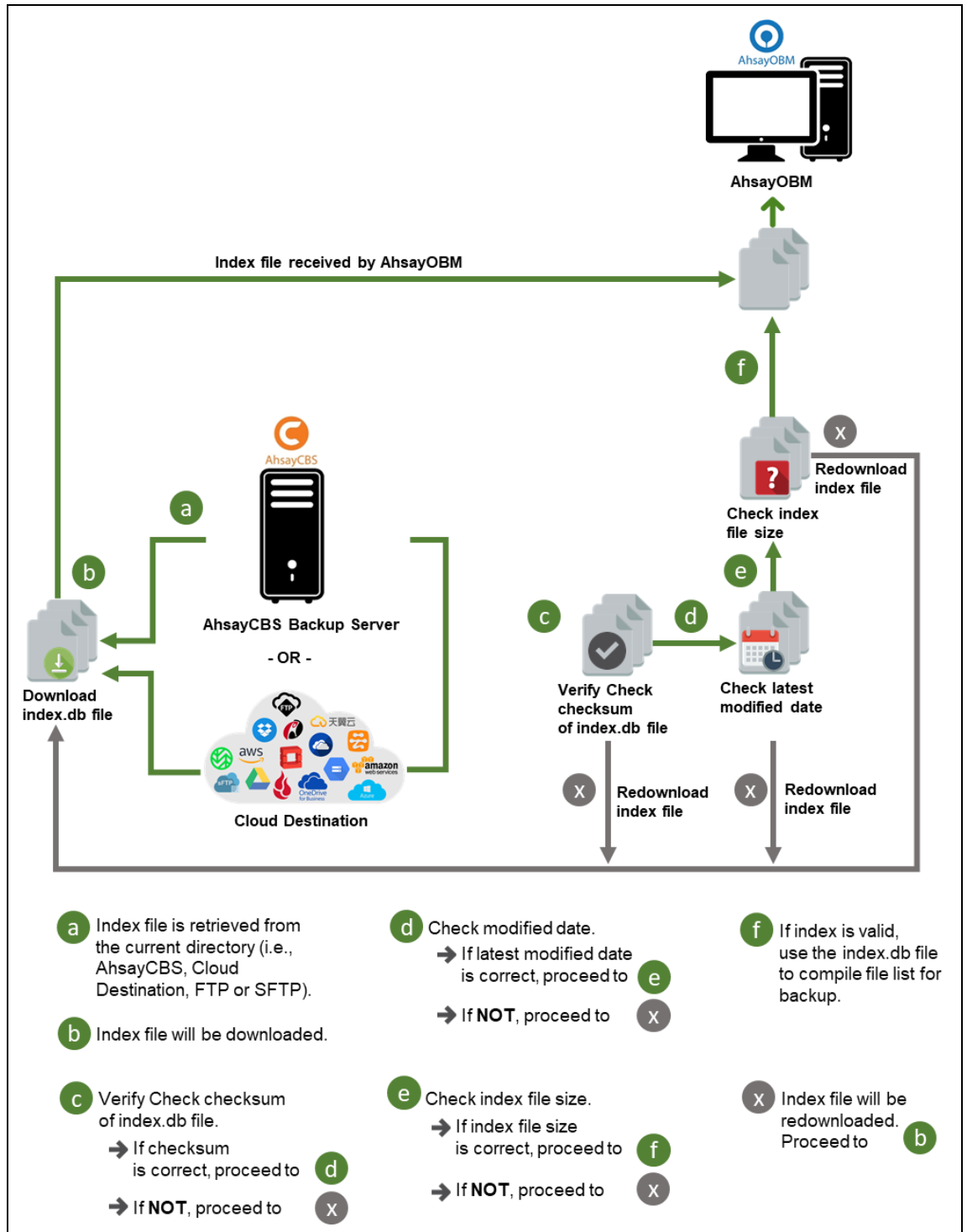Under certain conditions, the PDIC may not run strictly according to this formula. For example:

1. If AhsayOBM was upgraded to v8.5 (or above) from an older version v6, v7, or pre-8.3.6.0 version. In this case, the PDIC job will run on the first backup job after upgrade.

2. If backup jobs for a backup set are not run on a regular daily backup schedule (for example: on a weekly or monthly schedule), then the PDIC job will run if it detects that the previous PDIC job was run more than 7 days ago.
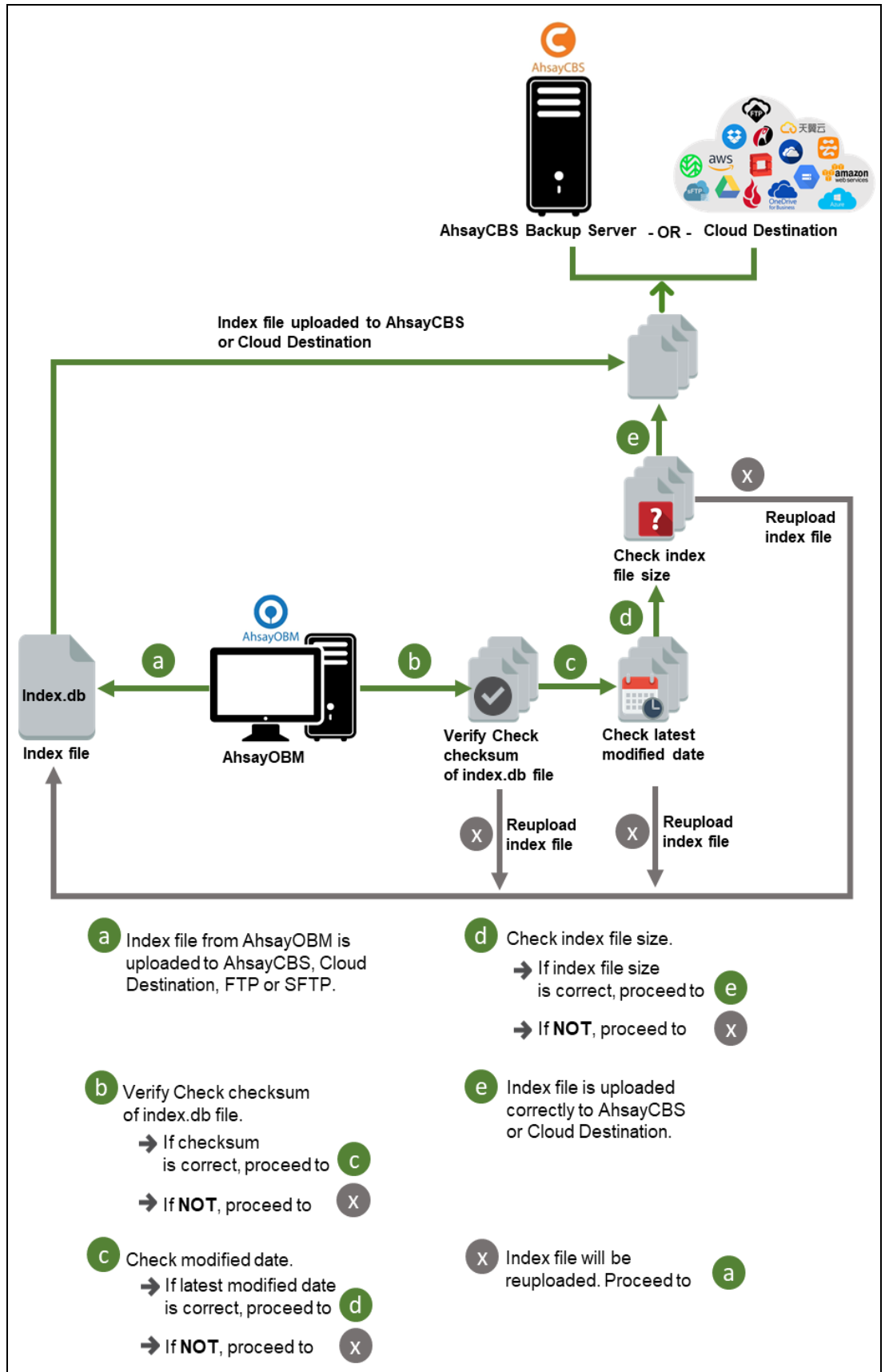

Start Periodic Data Integrity Check

a — **Checking index files which are more than 90 days old in the backup destination(s)**

y — **Removing index files from the backup destination(s) which are more than 90 days old**

b — **Checking outdated entries in the index files if they physically exist in the backup destination(s)**

z — **Removing outdated entries in the index files which do not physically exist in backup destination(s)**

No index-related issues found

c — **Storage Statistics recalculated**

d — **Periodic Data Integrity Check completed**

e — **Uploading index files with no issues to the current backup destination(s)**

f — **Continue backup job**

a Check the index files in the backup destination(s) to determine if they were more than 90 days old.
→ If **YES**, proceed to y
→ If **NO**, proceed to b

b Check the outdated entries in the index files for files and/or folders if they physically exist in the backup destination(s).
→ If **YES**, proceed to c
→ If **NO**, proceed to z

c Storage Statistics for Data area and Retention area usage will be recalculated.

d Periodic Data Integrity check is completed.

e Index files with no issues will be uploaded to the current backup destination(s).

f The backup job process will continue.

y Index files which are more than 90 days old will be removed from the backup destination(s).

z Outdated entries in the index files for files and/folders which do not physically exist in backup destination(s) will be removed.

7.4 Backup Set Index Handling Process

To minimize the possibility of index related issues affecting backups, each time index files are downloaded from and uploaded to backup destination(s); the file size, last modified date, and checksum is verified to ensure index file integrity.

7.4.1 Start Backup Job

7.4.2 Completed Backup Job

a   Index file from AhsayOBM is uploaded to AhsayCBS, Cloud Destination, FTP or SFTP.

b   Verify Check checksum of index.db file.
→ If checksum is correct, proceed to c
→ If NOT, proceed to x

c   Check modified date.
→ If latest modified date is correct, proceed to d
→ If NOT, proceed to x

d   Check index file size.
→ If index file size is correct, proceed to e
→ If NOT, proceed to x

e   Index file is uploaded correctly to AhsayCBS or Cloud Destination.

x   Index file will be reuploaded. Proceed to a

7.5 Data Validation Check Process

As an additional measure to ensure that all files transferred to the backup destination(s) are received and saved correctly, both the number of 16 or 32 MB data block files and the size of each block file are checked again after the files are transferred.
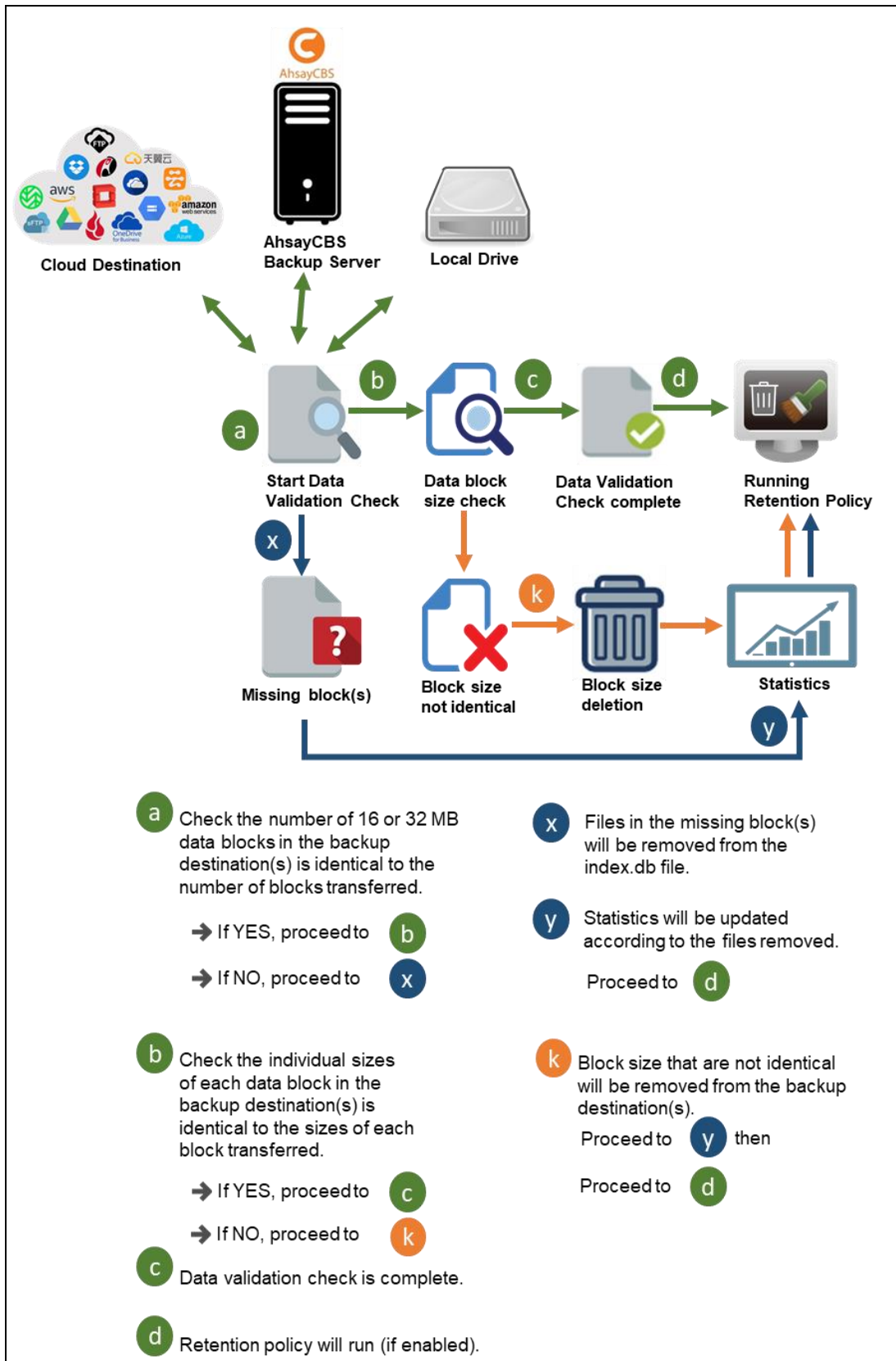
8 Running Backup Jobs

8.1 Login to AhsayOBM

Log in to AhsayOBM according to the instructions in Ch. 5.1 Login to AhsayOBM.

8.2 Start a Manual Backup

1. Click the **Backup** icon on the AhsayOBM main interface.

2. Select the Oracle database backup set which you would like to start a manual backup on.
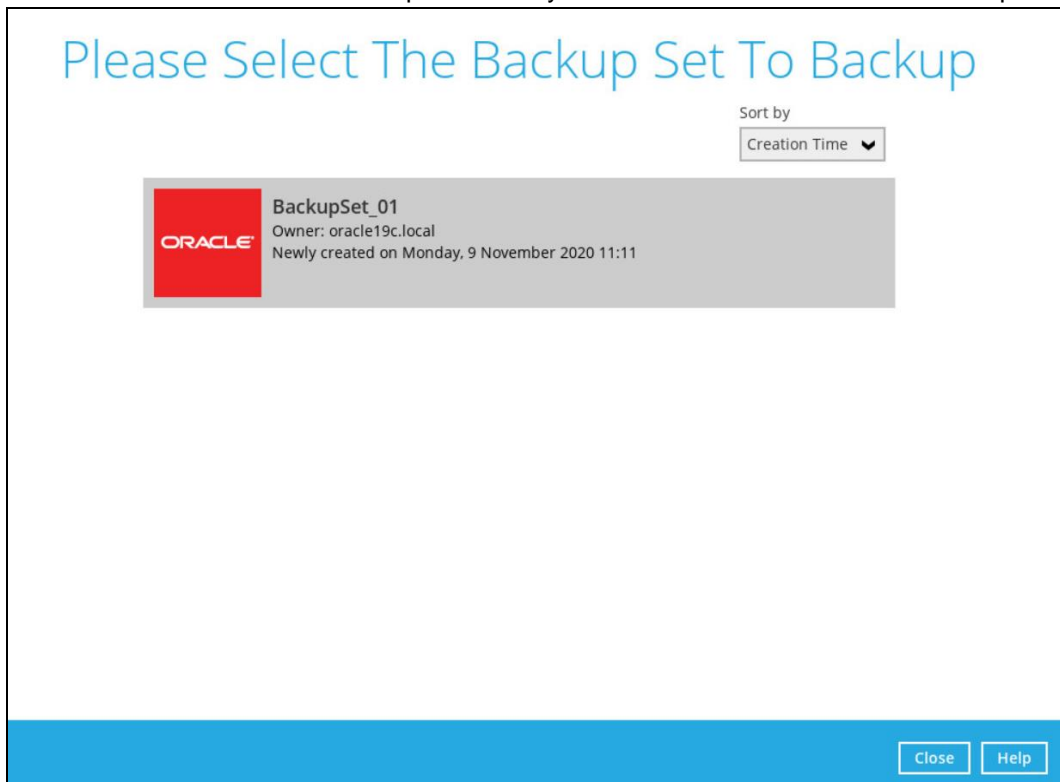
3. There are two (2) types of backup mode in an Oracle database backup set:

- **Database** – this type of backup includes Tablespaces, Control and Init File, and Archived Log Files. To see the steps during a database backup job, please refer to Ch. 7.1 Overview on the Database Backup Process.

- **Archived Log** – this type of backup is for archived log files. To see the steps during an archived log backup job, please refer to Ch. 7.2 Overview on the Archived Log Backup Process.
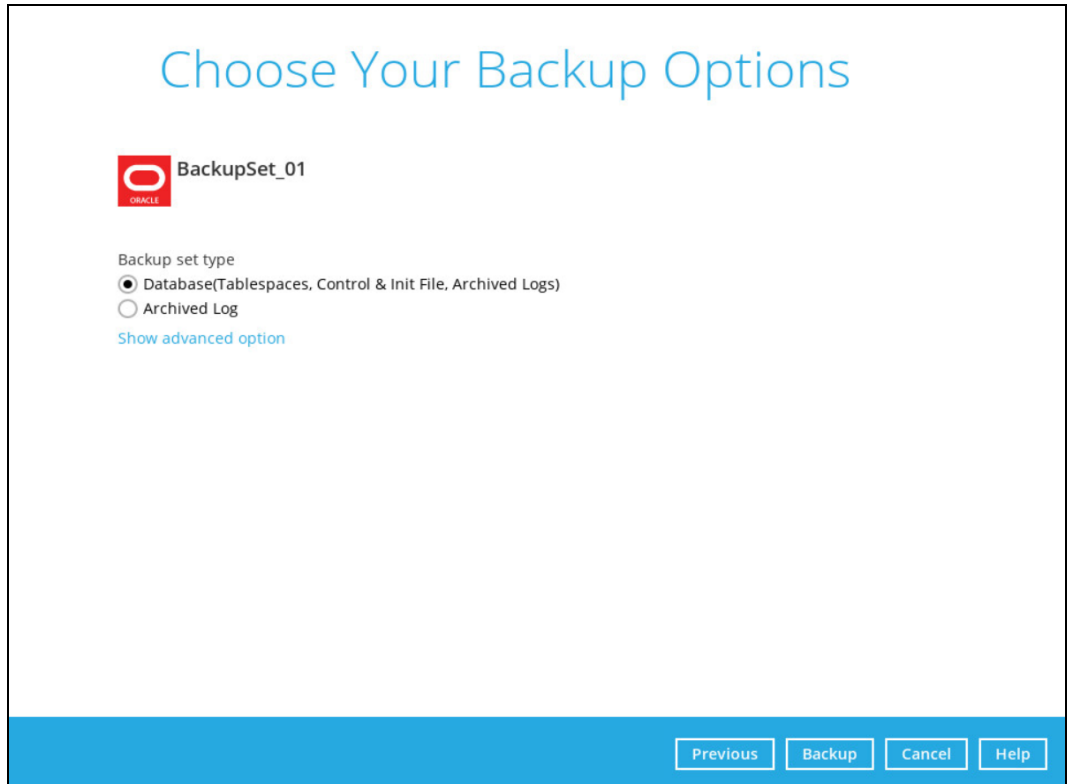
To modify the In-File Delta type, Destinations, or Run Retention Policy Settings before running a backup, click the **show advanced option** link.
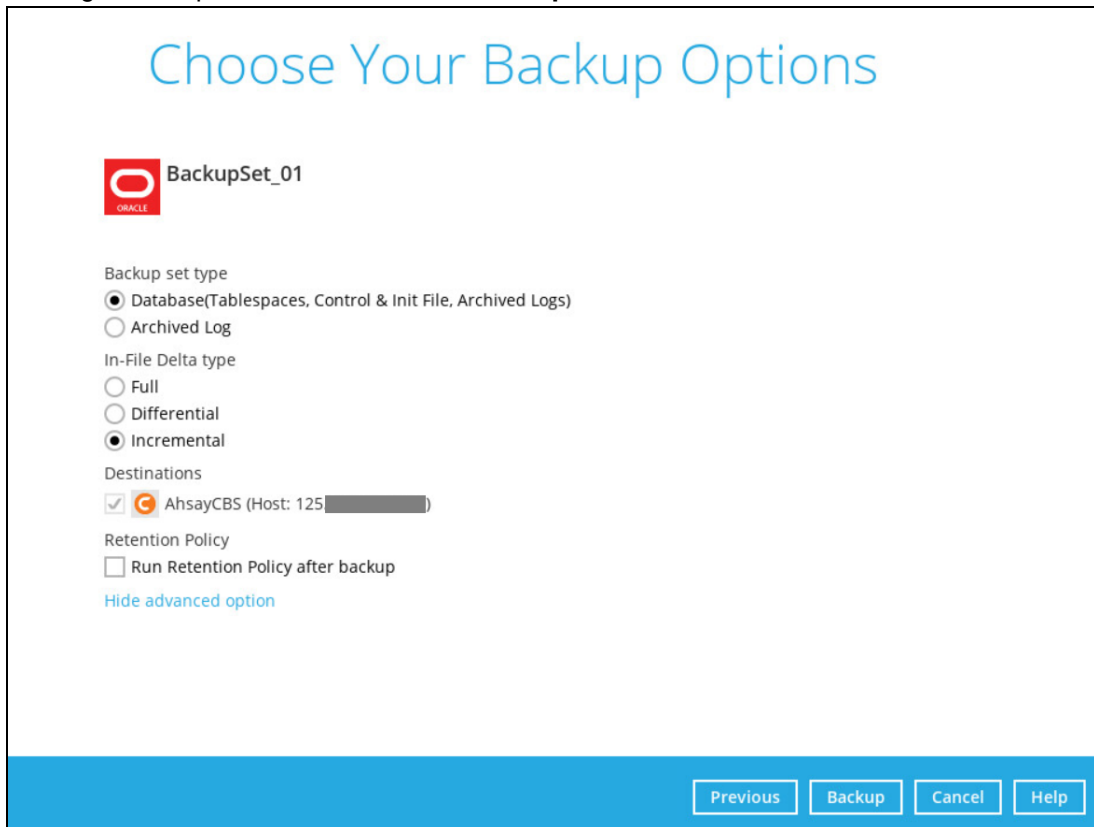
4. Click **Backup** to start the backup job.
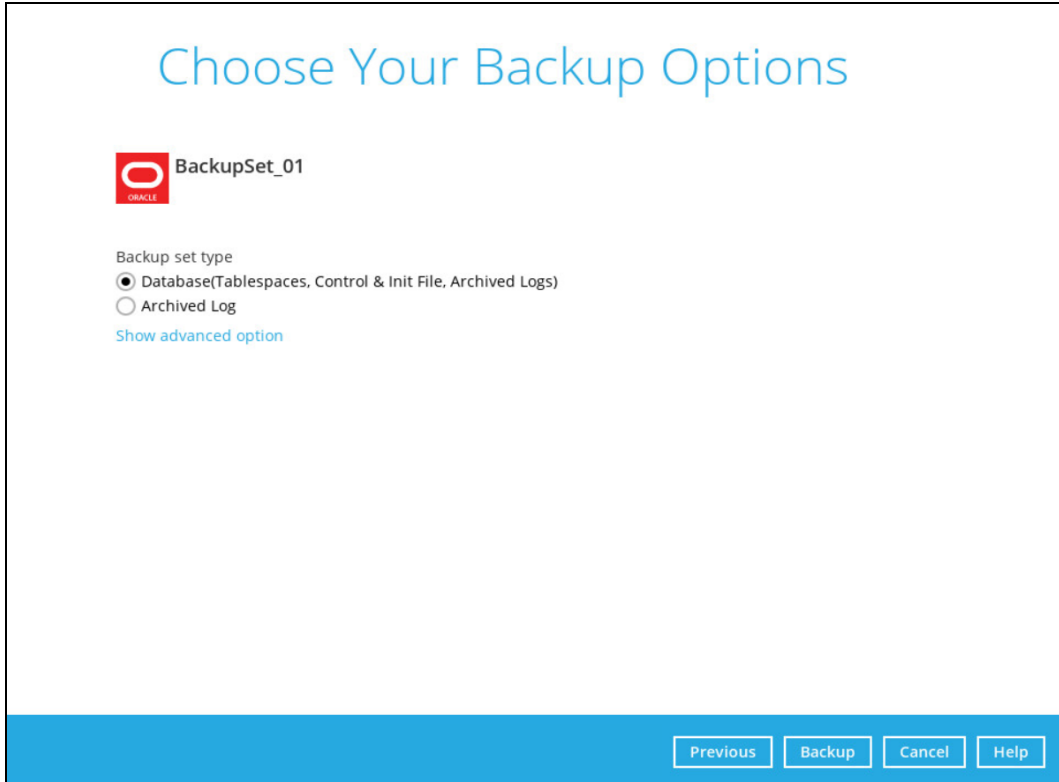
5. Backup job is completed successfully.
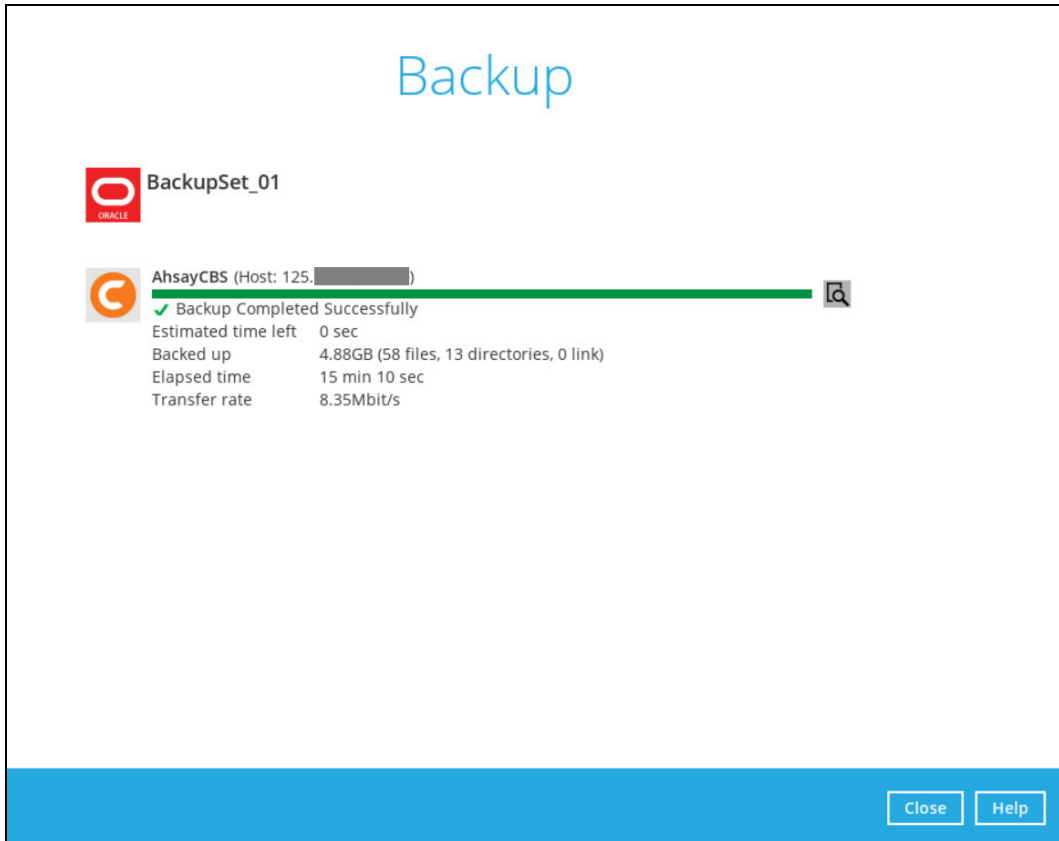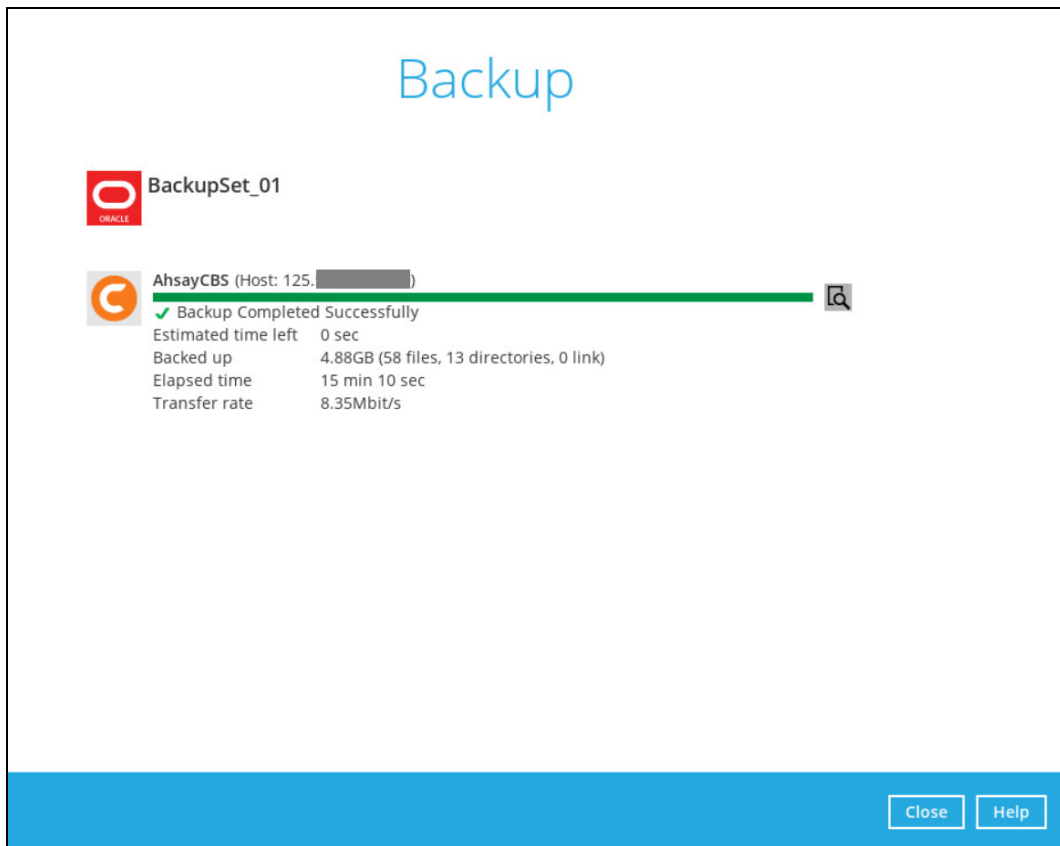
8.3 Configure Backup Schedule for Automated Backup

1. Click the **Backup Sets** icon on the AhsayOBM main interface.
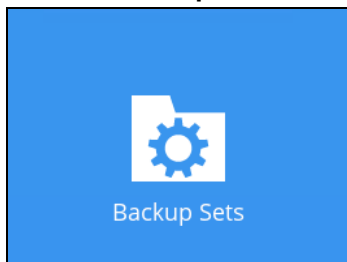
2. Select the backup set that you would like to create a backup schedule for.
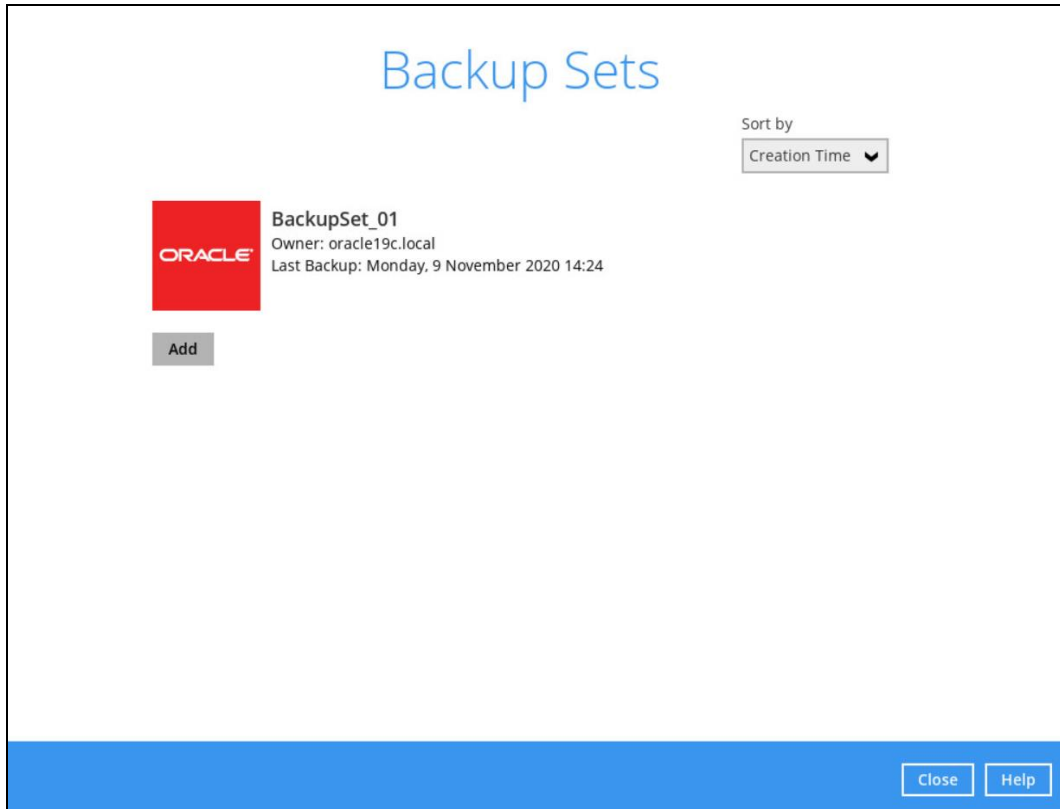
3. Go to the **Backup Schedule** tab.
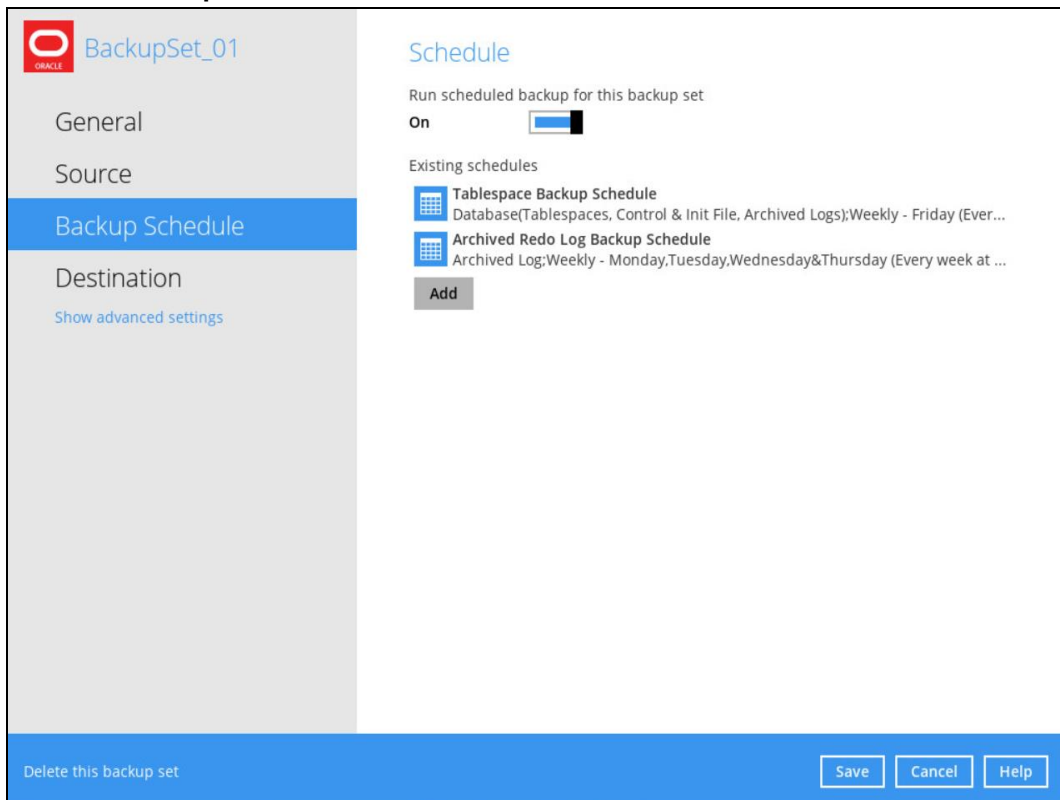
4. To modify an existing schedule, click the backup schedule to be modified. Or click the **Add** button to add a new one.

5. In the **New Backup Schedule** window, configure the following settings:

- **Name** – the name of the backup schedule

- **Backup set type** – the type of backup mode (i.e., Database and Archived Log)

- **Type** – the type of backup schedule. There are four (4) different types of backup schedule: Daily, Weekly, Monthly and Custom

  - **Daily** – the time of the day or interval in minutes/hours when the backup job will run

  - **Weekly** – the day of the week and the time of the day or interval in minutes/hours when the backup job will run

Monthly – the day of the month and the time of that day which the backup job will run

Custom – a specific date and the time of that date when the backup job will run

- **Start backup** – the start time of the backup job

  ▶ **at** – this option will start a backup job <u>at a specific time</u>

  ▶ **every** – this option will start a backup job <u>in intervals of minutes or hours</u>

Here is an example of a backup set that has a periodic and normal backup schedule.

<table>
<tr><td align="center">*Figure 1.1*</td><td align="center">*Figure 1.2*</td></tr>
</table>

Figure 1.1 – Periodic backup schedule runs every 4 hours from Monday – Friday during business hours for Archived Log backup

Figure 1.2 – Normal backup schedule runs at 21:00 or 9:00 PM every Sunday during non-business hours for Database backup

- **Stop** – the stop time of the backup job. This only applies to schedules with start backup "at" and is not supported for periodic backup schedule (start backup "every")

  - **until full backup completed** – this option will stop a backup job once it is complete. This is the configured stop time of the backup job by default.

  - **after (defined no. of hrs.)** – this option will stop a backup job after a certain number of hours regardless of whether the backup job has completed or not. This can range from 1 to 24 hrs.

    The number of hours must be enough to complete a backup of all files in the backup set. For small files in a backup, if the number of hours is not enough to back up all files, then the outstanding files will be backed up in the next backup job. However, if the backup set contains large files, this may result in partially backed up files.

    For example, if a backup has 100GB file size which will take approximately 15 hours to complete on your environment, but you set the "stop" after 10 hours, the file will be partially backed up and cannot be restored. The next backup will upload the files from scratch again.

    The partially backed up data will have to be removed by running the data integrity check.

    As a general rule, it is recommended to review this setting regularly as the data size on the backup machine may grow over time.

- **Run Retention Policy after backup** – if enabled, the AhsayOBM will run a retention policy job to remove files from the backup destination(s) which have exceeded the retention policy after performing a backup job

6. Before closing the Backup Schedule menu, click the **Save** button to apply the backup schedule settings.

9 Restoring Backup for Oracle Database Server

9.1 Restoring Data

There are three (3) restore options to choose from in Linux GUI mode:

- **Original location** – AhsayOBM will restore the database(s) from the backup destination and apply them to the original production Oracle instance.

- **Alternate location** – AhsayOBM will restore the database(s) from the backup destination and apply them to either the original Oracle instance or another Oracle instance on the production machine. This option can also be used to clone a database by changing the database name.

- **Restore raw file** – AhsayOBM will restore the Oracle database files to a location on the local machine, which then can be copied to another Oracle server on another machine for recovery.

  The **Restore Raw File** option is for advanced Oracle database administrators and should only be used if you have in-depth knowledge and understanding of Oracle database engine, Oracle database schema, knowledge of the database server and network infrastructure. Therefore, it is not recommended to use this restore option as there is need to utilize additional Oracle techniques and scripts to facilitate a manual database restore.

  Please refer to the following article of Oracle Database Backup and Recovery User's Guide for details:

  Oracle 19c
  https://docs.oracle.com/en/database/oracle/oracle-database/19/bradv/index.html

  Oracle 18c
  https://docs.oracle.com/en/database/oracle/oracle-database/18/bradv/index.html

9.2 Restore to Original Location

This feature is used to restore files from your backup destination and automatically apply them to the Oracle database server in the original location.

1. TNS listener service must be started to allow connections to the Oracle database server for the restore process. To check if the TNS listener service is running, use the *lsnrctl status* command. If the TNS listener service is not started, use the *lsnrctl start* command to start the service.

   Example: A running TNS Listener service on Oracle 19c.

```
$ lsnrctl status

LSNRCTL for Linux: Version 19.0.0.0.0 - Production on 05-NOV
2020 11:33:44

Copyright (c) 1991, 2019, Oracle.  All rights reserved.

Connecting to
 (DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=oracle19c.local)(POR
 T=1521)))
STATUS of the LISTENER
```

```
------------------------
Alias                    LISTENER
Version                  TNSLSNR for Linux: Version 19.0.0.0.0
 - Production
Start Date               03-NOV-2020 12:13:24
Uptime                   1 days 23 hr. 20 min. 20 sec
Trace Level              off
Security                 ON: Local OS Authentication
SNMP                     OFF
Listener Parameter File
 /u01/app/oracle/product/19.0.0/dbhome_1/network/admin/listener
 .ora
Listener Log File
 /u01/app/oracle/diag/tnslsnr/oracle19c/listener/alert/log.xml
Listening Endpoints Summary...

  (DESCRIPTION=(ADDRESS=(PROTOCOL=tcp)(HOST=oracle19c.local)(POR
 T=1521)))
    (DESCRIPTION=(ADDRESS=(PROTOCOL=ipc)(KEY=EXTPROC1521)))
Services Summary...
Service "86b637b62fdf7a65e053f706e80a27ca" has 1 instance(s).
   Instance "cdb1", status READY, has 1 handler(s) for this
 service...
Service "8886b84fb1e0709de053631e100a76ed" has 1 instance(s).
   Instance "cdb1", status READY, has 1 handler(s) for this
 service...
Service "cdb1" has 1 instance(s).
   Instance "cdb1", status READY, has 1 handler(s) for this
 service...
Service "cdb1XDB" has 1 instance(s).
   Instance "cdb1", status READY, has 1 handler(s) for this
 service...
Service "pdb1" has 1 instance(s).
   Instance "cdb1", status READY, has 1 handler(s) for this
 service...
The command completed successfully
```

NOTE: The values shown are just examples and might be different on your Oracle instance.

2. Run the `sqlplus / as sysdba` command to verify if the Oracle service is active.

The following is just an example after an Oracle instance failure due to corrupted data and/or configuration files. It might be different on your Oracle instance.

```
$ sqlplus / as sysdba

SQL*Plus: Release 19.0.0.0.0 - Production on Mon Nov 9 15:23:12
2020
Version 19.3.0.0.0

Copyright (c) 1982, 2019, Oracle.  All rights reserved.

Connected to an idle instance.
```

3. On the AhsayOBM main interface, click the **Restore** icon.

Restore

4. Select the backup set that you would like to restore the Oracle database from.

Please Select The Backup Set To Restore

Sort by

Creation Time ▼

ORACLE

BackupSet_01
Owner: oracle19c.local
Last Backup: Monday, 9 November 2020 14:24

Close   Help

5. Select the destination storage that contains the Oracle database(s) that you would like to restore from.

Select From Where To Restore

6. Select the database(s) that you would like to restore. You can also choose to restore backed up database from a specific backup job using the **Select what to restore** drop-down menu. Click **Next** to proceed.

Select Your Databases To Be Restored
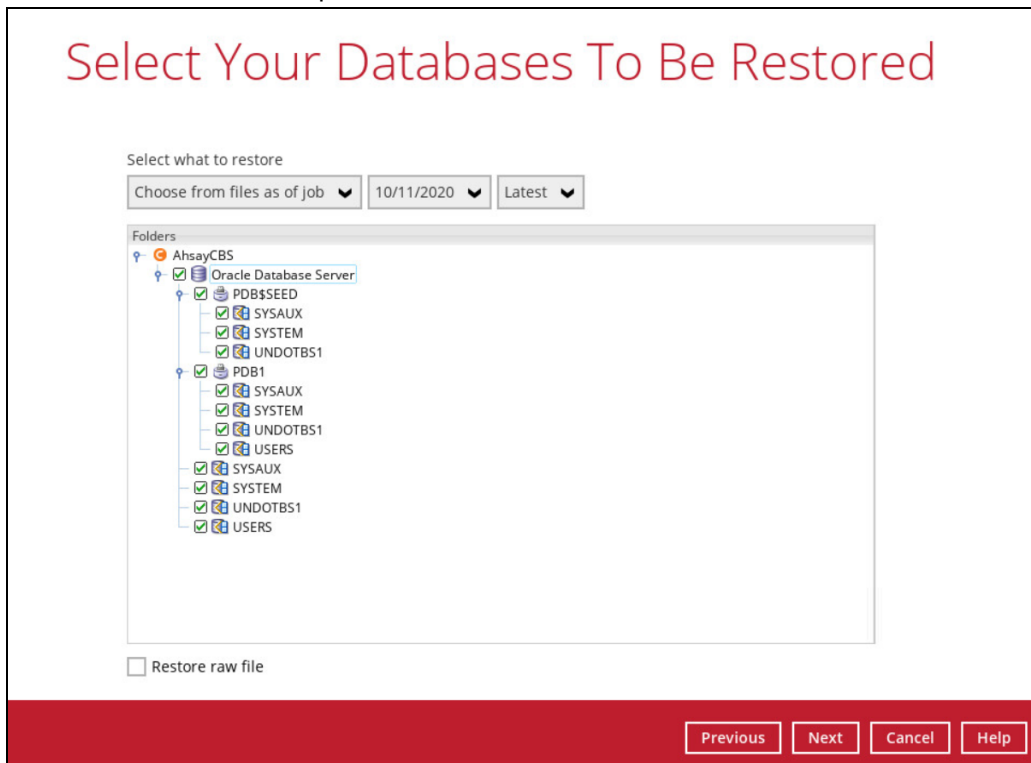
7. Choose **Original location** as where the database(s) will be restored.

If you would like to enable the **Verify checksum of in-file delta files during restore** setting, click the **Show advanced option** link.

8. Make sure that the temporary directory path is correct. To change its location, click **Browse** then click **OK** to select. Click **Restore** to start the restore process.

9. When this pop-up message is displayed, click **Yes** to continue.
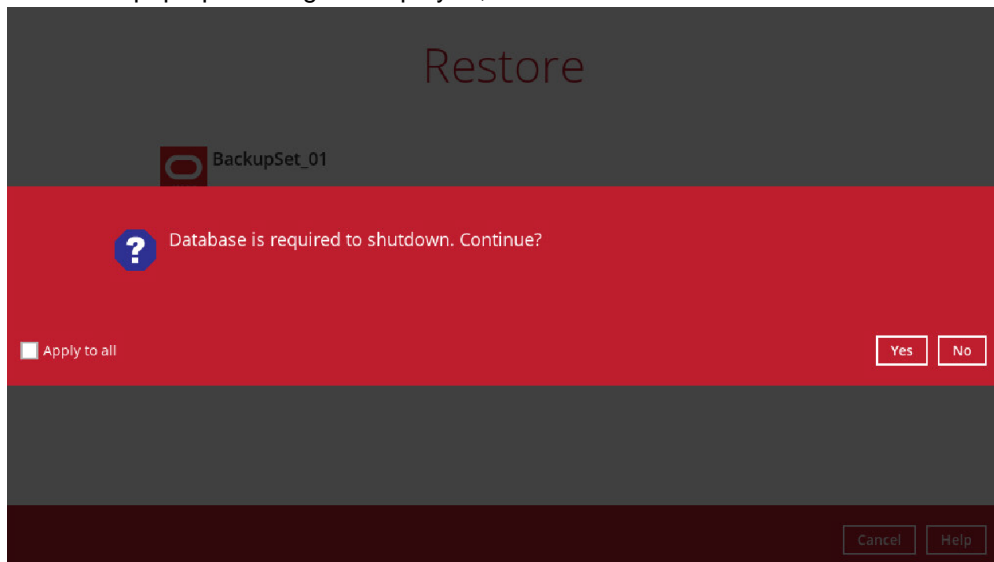
10. Restore job has completed successfully.
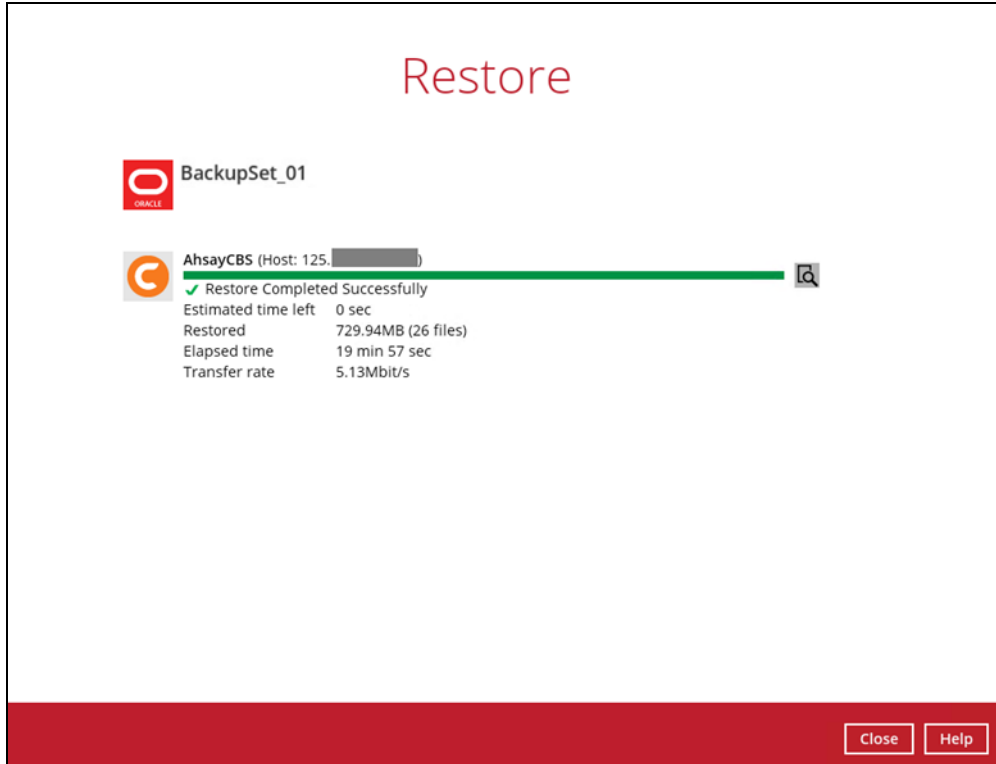
11. After the restore job is completed, verify if the Oracle database instance has been restored using the following SQL query to verify if the instance is online.

```
$ sqlplus / as sysdba

SQL*Plus: Release 19.0.0.0.0 - Production on Thu Nov 5 11:32:52
2020

Version 19.3.0.0.0

Copyright (c) 1982, 2019, Oracle.  All rights reserved.

Connected to:

Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 -
Production

Version 19.3.0.0.0

SQL> select instance from v$thread;

INSTANCE

--------------------------------------------------------------

cdb1

SQL>
```

9.3 Restore to Alternate Location

1. The folders used for the alternate location must be created using the Oracle user.

2. TNS listener service must be started to allow connections to the Oracle database server for the restore process. To check if the TNS listener service is running, use the `lsnrctl status` command. If the TNS listener service is not started, use the `lsnrctl start` command to start the service.

Example: A running TNS Listener service on Oracle 19c.

```
$ lsnrctl status

LSNRCTL for Linux: Version 19.0.0.0.0 - Production on 05-NOV
2020 11:33:44

Copyright (c) 1991, 2019, Oracle.  All rights reserved.

Connecting to
 (DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=oracle19c.local)(POR
 T=1521)))
STATUS of the LISTENER
------------------------
Alias                     LISTENER
Version                   TNSLSNR for Linux: Version 19.0.0.0.0
 - Production
Start Date                03-NOV-2020 12:13:24
Uptime                    1 days 23 hr. 20 min. 20 sec
Trace Level               off
Security                  ON: Local OS Authentication
SNMP                      OFF
Listener Parameter File
 /u01/app/oracle/product/19.0.0/dbhome_1/network/admin/listener
 .ora
Listener Log File
 /u01/app/oracle/diag/tnslsnr/oracle19c/listener/alert/log.xml
Listening Endpoints Summary...

 (DESCRIPTION=(ADDRESS=(PROTOCOL=tcp)(HOST=oracle19c.local)(POR
 T=1521)))
  (DESCRIPTION=(ADDRESS=(PROTOCOL=ipc)(KEY=EXTPROC1521)))
Services Summary...
Service "86b637b62fdf7a65e053f706e80a27ca" has 1 instance(s).
  Instance "cdb1", status READY, has 1 handler(s) for this
 service...
Service "8886b84fb1e0709de053631e100a76ed" has 1 instance(s).
  Instance "cdb1", status READY, has 1 handler(s) for this
 service...
Service "cdb1" has 1 instance(s).
  Instance "cdb1", status READY, has 1 handler(s) for this
 service...
Service "cdb1XDB" has 1 instance(s).
  Instance "cdb1", status READY, has 1 handler(s) for this
 service...
Service "pdb1" has 1 instance(s).
```

```
  Instance "cdb1", status READY, has 1 handler(s) for this
 service...
The command completed successfully
```

NOTE: The values shown are just examples and might be different on your Oracle instance.

3. Run the *sqlplus / as sysdba* command to verify if the Oracle service is active.

The following is just an example after an Oracle instance failure due to corrupted data and/or configuration files. It might be different on your Oracle instance.
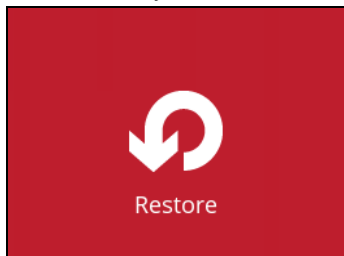
```
$ sqlplus / as sysdba

SQL*Plus: Release 19.0.0.0.0 - Production on Mon Nov 9 15:23:12
2020
Version 19.3.0.0.0

Copyright (c) 1982, 2019, Oracle.  All rights reserved.

Connected to an idle instance.
```

4. On the AhsayOBM main interface, click the **Restore** icon.

5. Select the backup set that you would like to restore the Oracle database from.

6. Select the destination storage that contains the Oracle database(s) that you would like to restore from.

7. Select the database(s) that you would like to restore, then click **Next** to proceed.

8. Choose **Alternate location** as where the database(s) will be restored.

If you would like to enable the **Verify checksum of in-file delta files during restore** setting, click the **Show advanced option** link.

9. Configure the following settings in the **Alternate database** screen:

- **Oracle Home** – where the Oracle_Home path is located. This is already set to the location of the Oracle_Home by default.

- **Host** – this value is set to 127.0.0.1.

- **Port** – the new port number of the alternate Oracle database instance.

- **SID** – the new SID for the alternate Oracle database instance.

  NOTE: If a restore will be performed to an alternate location, it is required to change the Oracle SID and port number.

- **Password** – the password for the system user account in the new database.

  NOTE: If password complexity is enabled on the Oracle instance, ensure that the password you will enter complies fully with the password complexity requirements.

  Otherwise, a restore error message will be shown due to a failed password complexity and the restore process will not be completed. Please refer to Appendix A for more details.

Once configured, click **Next** to proceed.

10. Once the Oracle database instance has been modified, it will reflect on the original **Database File Locations** automatically. Click **Next** to proceed.

11. Select the path of the **Recovery Location**. Click **Next** to proceed.

12. Make sure that the temporary directory path is correct. To change its location, click **Browse** then click **OK** to select. Click **Restore** to start the restore process.
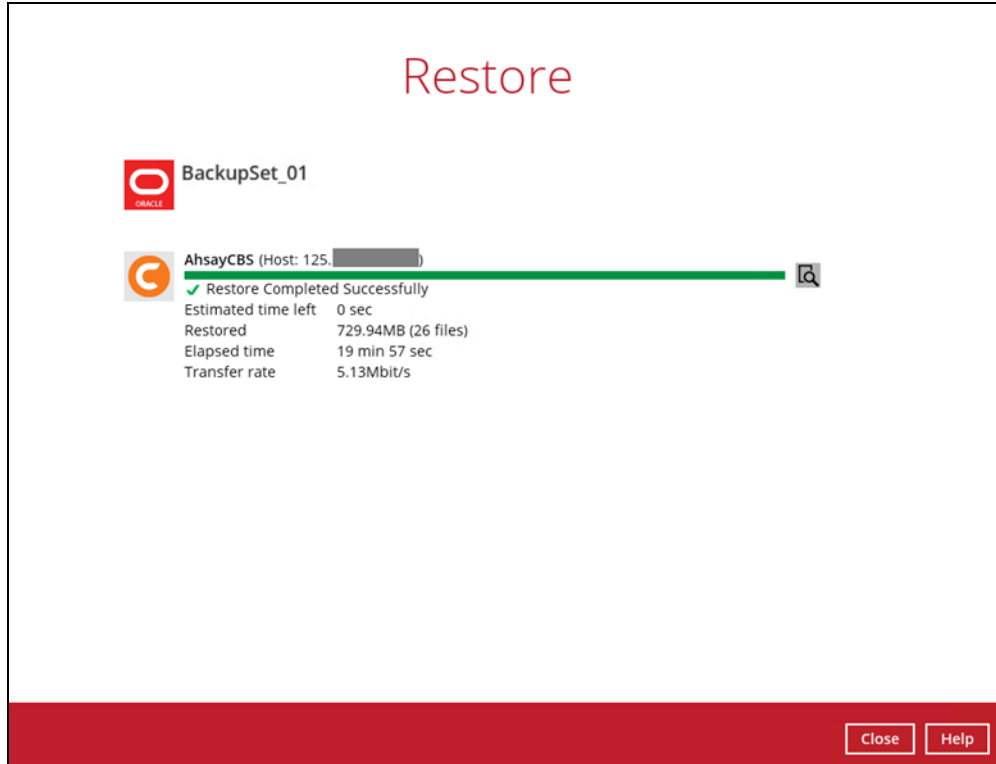
13. Restore job has completed successfully.

14. After the restore job is completed, verify if the Oracle database instance has been restored using the following SQL query to check if the instance is online.

```
$ sqlplus / as sysdba

SQL*Plus: Release 19.0.0.0.0 - Production on Thu Nov 5 11:32:52
2020

Version 19.3.0.0.0

Copyright (c) 1982, 2019, Oracle.  All rights reserved.

Connected to:

Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 -
Production

Version 19.3.0.0.0

SQL> select instance from v$thread;

INSTANCE

-------------------------------------------------------------

orcl

SQL>
```

9.4 Restore Raw File

This feature is used to restore the Oracle database(s) from your storage destination to a location on disk and manually recover the databases.

1. TNS listener service must be started to allow connections to the Oracle database server for the restore process. To check if the TNS listener service is running, use the *lsnrctl status* command. If the TNS listener service is not started, use the *lsnrctl start* command to start the service.

Example: A running TNS Listener service on Oracle 19c.

```
$ lsnrctl status

LSNRCTL for Linux: Version 19.0.0.0.0 - Production on 05-NOV
2020 11:33:44

Copyright (c) 1991, 2019, Oracle.  All rights reserved.

Connecting to
 (DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=oracle19c.local)(POR
 T=1521)))
STATUS of the LISTENER
------------------------
Alias                     LISTENER
Version                   TNSLSNR for Linux: Version 19.0.0.0.0
 - Production
Start Date                03-NOV-2020 12:13:24
Uptime                    1 days 23 hr. 20 min. 20 sec
Trace Level               off
Security                  ON: Local OS Authentication
SNMP                      OFF
Listener Parameter File
 /u01/app/oracle/product/19.0.0/dbhome_1/network/admin/listener
 .ora
Listener Log File
 /u01/app/oracle/diag/tnslsnr/oracle19c/listener/alert/log.xml
Listening Endpoints Summary...

 (DESCRIPTION=(ADDRESS=(PROTOCOL=tcp)(HOST=oracle19c.local)(POR
 T=1521)))
  (DESCRIPTION=(ADDRESS=(PROTOCOL=ipc)(KEY=EXTPROC1521)))
Services Summary...
Service "86b637b62fdf7a65e053f706e80a27ca" has 1 instance(s).
  Instance "cdb1", status READY, has 1 handler(s) for this
 service...
Service "8886b84fb1e0709de053631e100a76ed" has 1 instance(s).
  Instance "cdb1", status READY, has 1 handler(s) for this
 service...
Service "cdb1" has 1 instance(s).
  Instance "cdb1", status READY, has 1 handler(s) for this
 service...
Service "cdb1XDB" has 1 instance(s).
  Instance "cdb1", status READY, has 1 handler(s) for this
 service...
```

```
Service "pdb1" has 1 instance(s).
  Instance "cdb1", status READY, has 1 handler(s) for this
 service...
The command completed successfully
```

NOTE: The values shown are just examples and might be different on your Oracle instance.

2. Run the *sqlplus / as sysdba* command to verify if the Oracle service is active.

The following is just an example after an Oracle instance failure due to corrupted data and/or configuration files. It might be different on your Oracle instance.
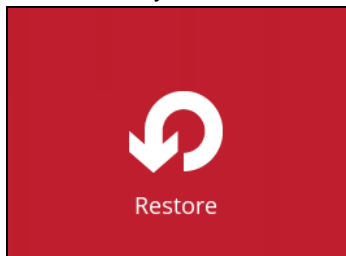
```
$ sqlplus / as sysdba

SQL*Plus: Release 19.0.0.0.0 - Production on Mon Nov 9 15:23:12
2020
Version 19.3.0.0.0

Copyright (c) 1982, 2019, Oracle.  All rights reserved.

Connected to an idle instance.
```

3. On the AhsayOBM main interface, click the **Restore** icon.

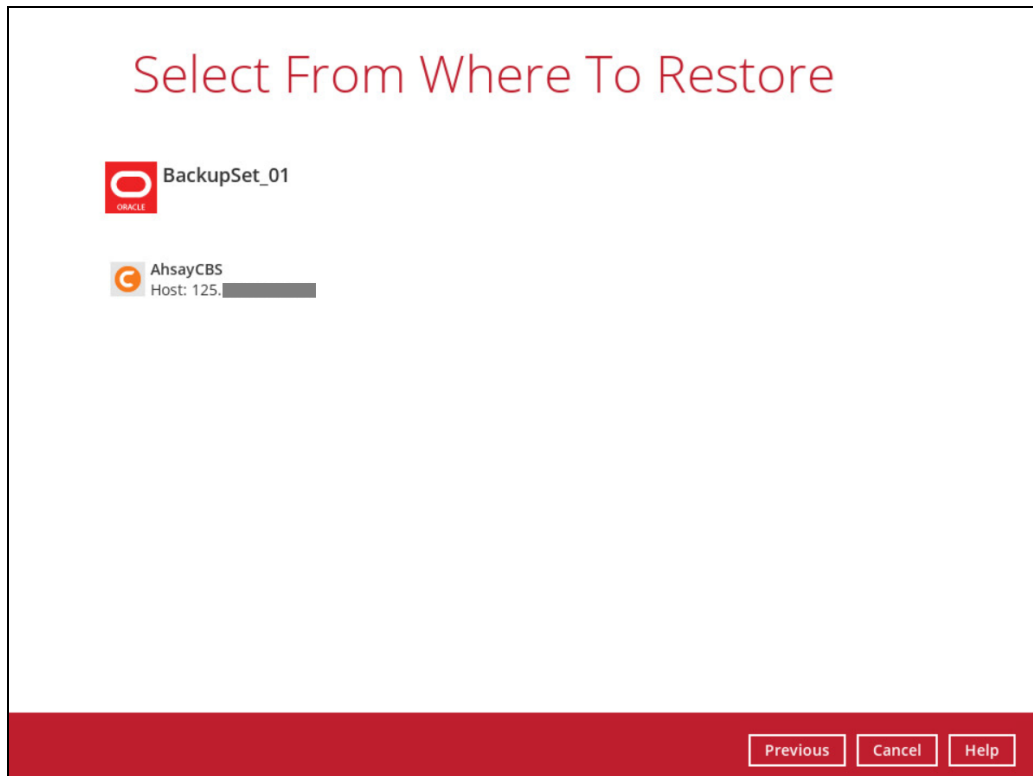4. Select the backup set that you would like to restore the Oracle database from.

5. Select the destination storage that contains the Oracle database(s) that you would like to restore from.

6. Click the **Restore raw file** option then select the Oracle database(s) to be restored. Click **Next** to proceed.

7. Click **Browse** to select the location on the local machine where you wish to restore the Oracle database(s) to. Click **Next** to proceed.

If you would like to enable the **Verify checksum of in-file delta files during restore** setting, click the **Show advanced option** link.
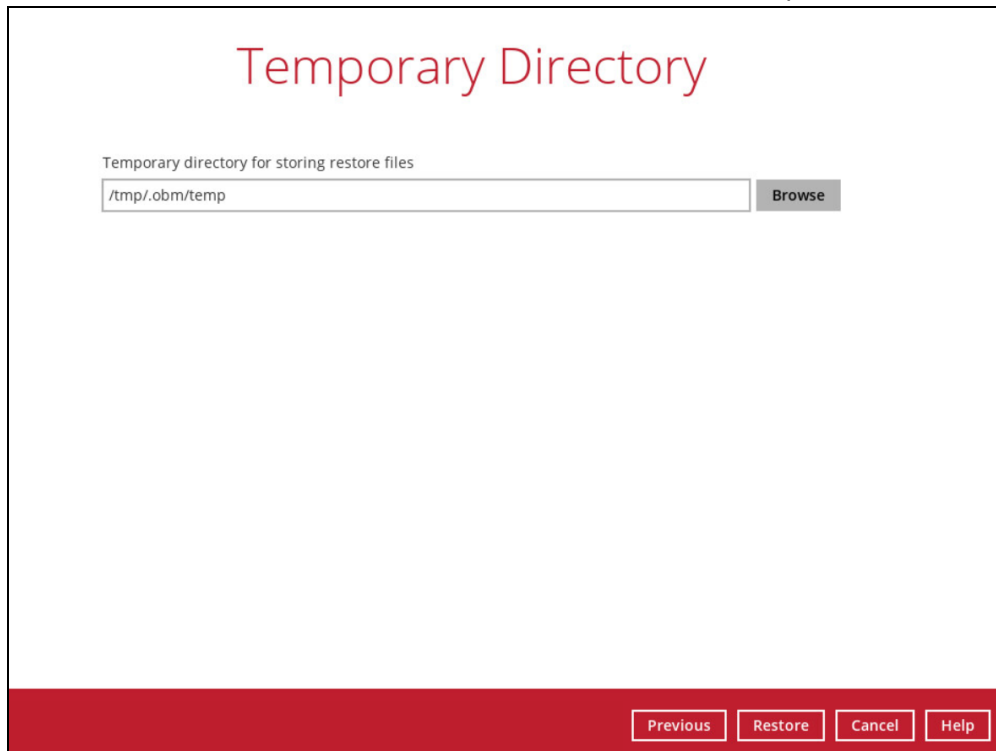
8. Make sure that the temporary directory path is correct. To change its location, click **Browse** then click **OK** to select. Click **Restore** to start the restore process.

Temporary Directory

Temporary directory for storing restore files

/tmp/.obm/temp   Browse

Previous | Restore | Cancel | Help

9. Restore job has completed successfully.

Restore

BackupSet_01

AhsayCBS (Host: 125.   )
✔ Restore Completed Successfully
Estimated time left   0 sec
Restored   729.94MB (26 files)
Elapsed time   19 min 57 sec
Transfer rate   5.13Mbit/s

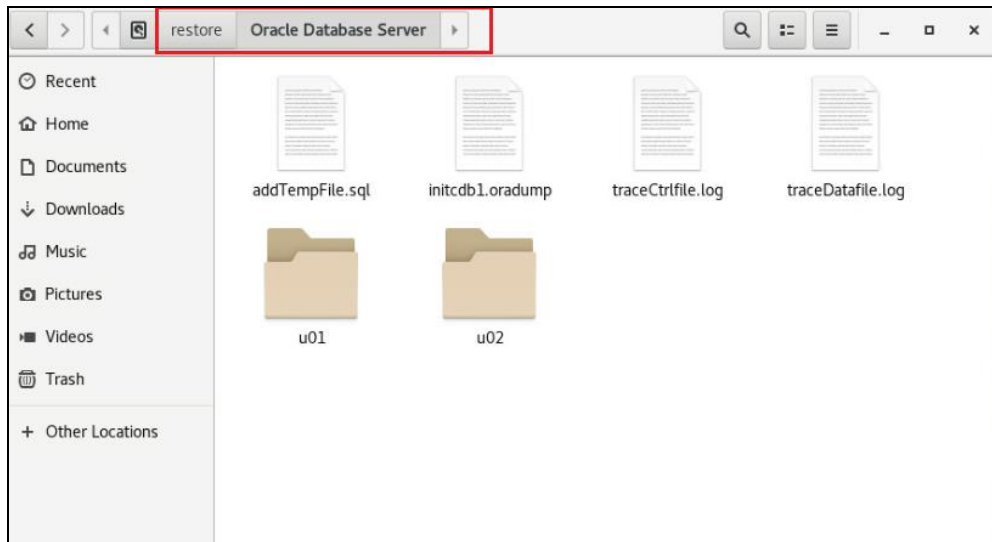Close | Help
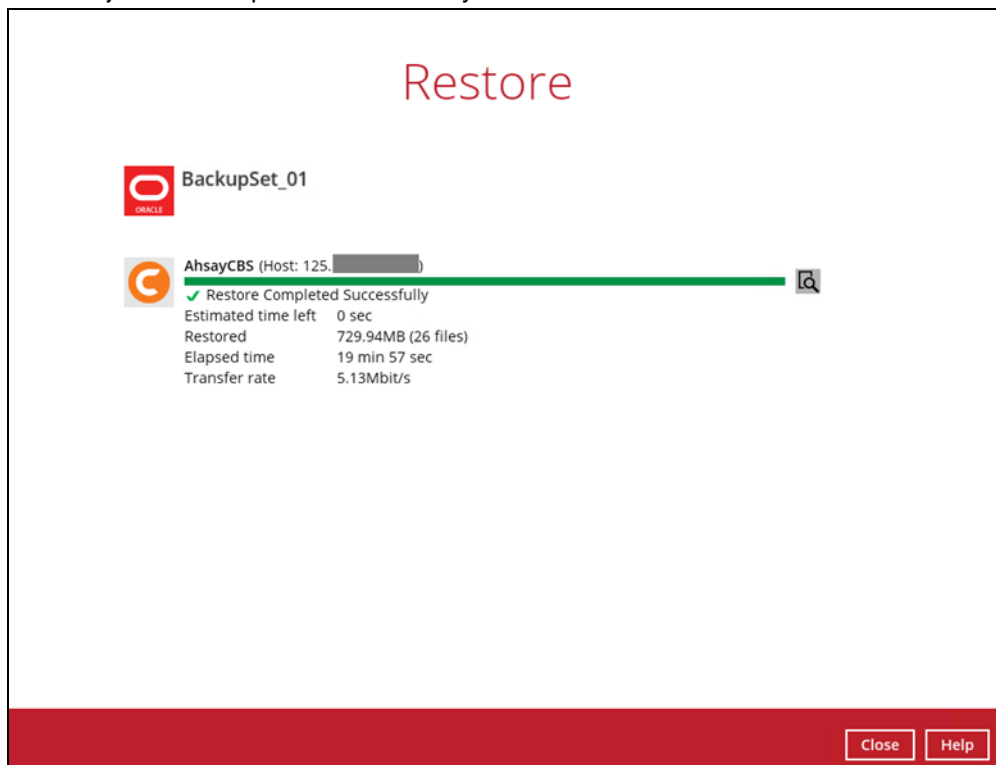
10. After the restore job is completed, verify if the Oracle database(s) have been restored. Go to the designated path on the local machine where you restored the Oracle database files to.

Example:

11. Recovering RAW Oracle databases

To recover RAW databases, please refer to the following article of Oracle Database Backup and Recovery User's Guide for details:

Oracle 19c
https://docs.oracle.com/en/database/oracle/oracle-database/19/bradv/index.html

Oracle 18c
https://docs.oracle.com/en/database/oracle/oracle-database/18/bradv/index.html

10 Contacting Ahsay

10.1 Technical Assistance

To contact Ahsay support representatives for technical assistance, visit the Partner Portal:
https://www.ahsay.com/partners/

Also use the Ahsay Wikipedia for resource such as Hardware Compatibility List, Software Compatibility List, and other product information:
https://wiki.ahsay.com/

10.2 Documentation

Documentations for all Ahsay products are available at:
https://www.ahsay.com/jsp/en/home/index.jsp?pageContentKey=ahsay_downloads_documentation_guides

You can send us suggestions for improvements or report on issues in the documentation by contacting us at:
https://www.ahsay.com/partners/

Please specify the specific document title as well as the change required/suggestion when contacting us.

Appendix

Appendix A   Example of Restore Log with Error Due to Enforced Password Complexity Requirements

The following log highlighted in red is an example of a common restore error message that may be shown during Restore to Alternate location if the password entered for the system user account in the Alternate Database screen is unable to comply with password complexity requirements.

```
[2021/03/01 17:29:24] [cbs] info,"Start restore database from \"cdb1\" to
\"orcl\"",0,0,0,1614580626387,0,0
[2021/03/01 17:29:28] [erro] OPW-00029: Password complexity failed for
SYS user : Password must contain at least 1 special character.
[2021/03/01 17:29:28] [cbs] erro,OPW-00029: Password complexity failed
for SYS user : Password must contain at least 1 special
character.,0,0,0,1614580626387,0,0
[2021/03/01 17:29:28] [erro] [hV] Restore database fail., Reason = "New
password file fail"
[2021/03/01 17:29:28] [cbs] erro,"[hV] Restore database fail., Reason =
\"New password file fail\"",0,0,0,1614580626387,0,0
[2021/03/01 17:29:28] [erro] Restore completed with error(s)
[2021/03/01 17:29:28] [cbs]
end,RESTORE_STOP_SUCCESS_WITH_ERROR,0,0,0,1614580626387,0,0
```