Oracle® Cloud
Using Oracle Database Backup Cloud Service
## Contents

### Preface
- Audience: v
- Documentation Accessibility: v
- Related Resources: v
- Conventions: vi

### 1 Getting Started with Oracle Database Backup Cloud Service
- About Oracle Database Backup Cloud Service: 1-1
- About Backup and Recovery Using Oracle Database Backup Cloud Service: 1-2
- About the Oracle Database Cloud Backup Module for OCI: 1-2
- About the Oracle Database Cloud Backup Module for OCI Classic: 1-3
- Important Information About Oracle Database Backup Cloud Service Subscriptions: 1-3
- How to Begin with Oracle Database Backup Cloud Service Subscriptions: 1-3
- Frequently Asked Questions for Oracle Database Backup Cloud Service: 1-4

### 2 Administering Oracle Database Backup Cloud Service
- Typical Workflow for Administering Oracle Database Backup Cloud Service: 2-1
- Installing the Oracle Database Cloud Backup Module for OCI: 2-2
  - Before You Begin Installing Oracle Database Cloud Backup Module for OCI: 2-3
  - Supported Databases and Operating Systems: 2-4
  - Parameters to Run the Oracle Database Cloud Backup Module for OCI: 2-4
  - Downloading and Installing the Oracle Database Cloud Backup Module for OCI: 2-10
  - Files Created when Oracle Database Cloud Backup Module for OCI is Installed: 2-12
- Installing the Oracle Database Cloud Backup Module for OCI Classic: 2-13
  - Before You Begin Installing Oracle Database Cloud Backup Module for OCI Classic: 2-13
  - Parameters Used to Run the Oracle Database Cloud Backup Module for OCI Classic Installer: 2-14
  - Downloading and Installing the Oracle Database Cloud Backup Module for OCI Classic: 2-18
  - Files Created When the Oracle Database Cloud Backup Module for OCI Classic is Installed: 2-20
# Configuring Recovery Manager (RMAN) Settings

- Configuring Encryption for Backups  2-23
- Configuring Compression for Backups  2-23
- Management Interfaces for Cloud Backups  2-24
- Storing Backups in Custom Locations  2-24
- Configuring Automatic Archival to Oracle Cloud Infrastructure  2-26
- Configuring Automatic Archival to Oracle Cloud Infrastructure Classic  2-27
- Monitoring Your Storage Capacity  2-28

# Backing Up to Oracle Database Backup Cloud Service

- Backing Up to Oracle Database Backup Cloud Service  3-2
- Backing Up to Oracle Database Backup Cloud Service Using Password Encryption  3-2
- Backing Up to Oracle Database Backup Cloud Service Using Transparent Data Encryption (TDE)  3-3
- Backing Up to Oracle Database Backup Cloud Service Using Dual-Mode Encryption  3-4
- Backing Up from the Fast Recovery Area (FRA) to Oracle Database Backup Cloud Service  3-4

# Restoring Backups from Oracle Database Backup Cloud Service

- Performing General Restore and Recovery Operations  4-1
- Recovering Databases from Archive Storage  4-2
- Restoring to a New Database Host  4-3
- Creating a Data Guard Standby Database in Oracle Cloud  4-5

# Troubleshooting Oracle Database Backup Cloud Service

- Best Practices to Optimize Cloud Backup and Restore Rates  5-1
- Problems with Installing the Backup Module  5-2
- Problems with Backing Up and Restoring  5-5
- Problems with Connectivity  5-7
Preface

This document describes how to use Oracle Database Backup Cloud Service to back up Oracle databases to Oracle Cloud.

Topics:

• Audience
• Related Resources
• Conventions

Audience

This document is intended for administrators who want to use Oracle Database Backup Cloud Service to back up Oracle databases to Oracle Cloud.

It is assumed you know the following:

• Oracle Database concepts and basic database administration
• Recovery Manager (RMAN) concepts, usage, tasks, and commands
• The operating system environment under which you run Oracle Database

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Related Resources

For more information, see these Oracle resources:

• Database Backup on the Oracle Cloud website
  https://cloud.oracle.com/database_backup
• Oracle Database Backup Cloud Service FAQ (My Oracle Support Doc ID 1640149.1)
The following text conventions are used in this document:

<table>
<thead>
<tr>
<th>Convention</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>boldface</strong></td>
<td>Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.</td>
</tr>
<tr>
<td><em>italic</em></td>
<td>Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.</td>
</tr>
<tr>
<td>monospace</td>
<td>Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.</td>
</tr>
</tbody>
</table>
Getting Started with Oracle Database Backup Cloud Service

Oracle Database Backup Cloud Service is a cloud storage solution for storing Oracle Database backups. Here’s what you need to know to get started.

Topics

- About Oracle Database Backup Cloud Service
- About Backup and Recovery Using Oracle Database Backup Cloud Service
- About the Oracle Database Cloud Backup Module for OCI
- About the Oracle Database Cloud Backup Module for OCI Classic
- Important Information About Oracle Database Backup Cloud Service Subscriptions
- How to Begin with Oracle Database Backup Cloud Service Subscriptions
- Frequently Asked Questions for Oracle Database Backup Cloud Service

About Oracle Database Backup Cloud Service

Oracle Database Backup Cloud Service is a secure, scalable, on-demand storage solution for backing up Oracle databases to Oracle Cloud. The service complements your existing backup strategy by providing an off-site storage location in the public cloud.

To use Oracle Database Backup Cloud Service you’ll subscribe to the service, install the Oracle Database Cloud Backup Module, and configure your environment to send backups to the cloud. You can then use familiar Recovery Manager (RMAN) commands to perform backup, restore, recovery, and maintenance operations. You can also use other tools for your cloud backups. See Management Interfaces for Cloud Backups.

With Oracle Database Backup Cloud Service, cloud backups are always accessible over the Internet and are immediately available for recovery when needed. Data is replicated across multiple storage nodes, which protects against hardware failure and data corruption.

Additionally, Oracle Database Backup Cloud Service supports two Oracle Database optimizations:

- **RMAN backup encryption**
  
  Using RMAN encryption, your data is encrypted at the source, securely transmitted to the cloud, and securely stored in the cloud. The keys are kept at your site, not in the cloud.

- **All RMAN backup compression algorithms**
Using RMAN backup compression, you can conserve bandwidth and improve performance by reducing the size of backups before they're sent to the cloud for storage.

For licensing information about these optimizations, see Oracle Database Backup Cloud Service in Oracle Database Licensing Information User Manual.

Oracle Database Backup Cloud Service is used to store Oracle Database backups only. To store other types of data, use Oracle Storage Cloud Service. See About Oracle Storage Cloud Service in Using Oracle Storage Cloud Service.

Oracle Database Backup Cloud Service can also be used to back up and restore Oracle Database Cloud Service and Oracle Database Exadata Cloud Service deployments.

For instances created using the Oracle Database Cloud Service - Virtual Image service level, download the Oracle Database Cloud Backup Module and perform tasks as described in this document.

For Database Cloud Service (non-Virtual Image) and Exadata Cloud Service instances, instance images come with the backup module already installed, so you don't need to install the module, configure RMAN, and so on. For information about backup and recovery in this case, see Backing Up and Restoring Databases on Database Cloud Service in Using Oracle Database Cloud Service. For information about billing, see relevant details in How to Begin with Database Cloud Service Subscriptions in Using Oracle Database Cloud Service. For Exadata Cloud Service, see Backing Up and Restoring Databases on Exadata Cloud Service in Using Oracle Database Exadata Cloud Service.

About Backup and Recovery Using Oracle Database Backup Cloud Service

Oracle Database Backup Cloud Service is used to back up Oracle databases to Oracle Cloud. When required, database restore and recovery can be performed using the backups stored in Oracle Cloud.

Oracle Database Backup Cloud Service can create backups to:

- Oracle Cloud Infrastructure
  
  To create backups to Oracle Cloud Infrastructure, you must have a subscription to an Oracle Cloud Service and install the Oracle Database Cloud Backup Module for OCI.
  
- Oracle Cloud Infrastructure Classic
  
  To create backups to Oracle Cloud Infrastructure Classic, you must have a subscription to an Oracle Cloud Service and install the Oracle Database Cloud Backup Module for OCI Classic.

About the Oracle Database Cloud Backup Module for OCI

The Oracle Database Cloud Backup Module for OCI makes it possible to perform backups and restores with Oracle Cloud Infrastructure.
This module is a system backup to tape (SBT) interface that is integrated with Recovery Manager (RMAN). You can use standard RMAN commands to perform backup, restore, recovery, and maintenance operations.

You'll download the Oracle Database Cloud Backup Module for OCI 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 for OCI.

Installing and using the module requires your Oracle Cloud credentials. After the module is installed, the authentication keys are stored securely in the Oracle wallet and are used to authenticate the module’s interactions with Oracle Cloud Infrastructure Object Storage. Backups created using the Oracle Database Cloud Backup Module for OCI are stored in Oracle Cloud Infrastructure Object Storage.

About the Oracle Database Cloud Backup Module for OCI Classic

The Oracle Database Cloud Backup Module for OCI Classic makes it possible to perform cloud backups and restores with Oracle Cloud Infrastructure Classic.

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 for OCI Classic. Backups created using the Oracle Database Cloud Backup Module for OCI Classic are stored in Oracle Cloud Infrastructure Object Storage Classic.

Important Information About Oracle Database Backup Cloud Service Subscriptions

When you request a trial of Oracle Database Backup Cloud Service, you actually get a trial of Oracle Storage Cloud Service. Oracle Database Backup Cloud Service uses Oracle Storage Cloud Service to store cloud backups.

To try Oracle Database Backup Cloud Service, go to cloud.oracle.com/database_backup or cloud.oracle.com/database and click Try For Free.

For trials and paid subscriptions to Oracle Database Backup Cloud Service, the service is listed as Oracle Storage Cloud Service in Cloud Portal. Email from Oracle references Oracle Storage Cloud Service.

How to Begin with Oracle Database Backup Cloud Service Subscriptions

Here’s how to get started with Oracle Database Backup Cloud Service subscriptions.
1. Request a trial or purchase a subscription using any of the following methods:
   • Request a trial subscription to Oracle Database Backup Cloud Service. See Request and Manage Free Oracle Cloud Promotions in Getting Started with Oracle Cloud.
   • Purchase a paid subscription to Oracle Database Backup Cloud Service. See Buy a Nonmetered Subscription to an Oracle Cloud Service in Getting Started with Oracle Cloud or How Do I Sign Up? in Getting Started with Oracle Cloud for information about universal credits.

   Oracle Database Backup Cloud Service trials and paid subscriptions appear as Oracle Storage Cloud Service subscriptions. See Important Information About Oracle Database Backup Cloud Service Subscriptions.

2. Activate and verify the service. See Activate Your Order in Getting Started with Oracle Cloud.

3. Verify activation. See Verify That Your Services are Ready in Getting Started with Oracle Cloud.

4. **Important Step:** Select a data center for your service (you’ll see Set Replication Policy for Oracle Storage Cloud Service when you sign in to the Infrastructure Classic Console). See About Replication Policy for Your Object Storage Classic Instance in Using Oracle Storage Cloud Service.

   You don't need to create a storage container as mentioned in the procedure. A default storage container is created for you automatically when you install the backup module used by Oracle Database Backup Cloud Service.

   If you enable georeplication, you will be billed for the capacity utilized in both the source and target data centers.

   The replication policy must be set before you run the backup module installer. Otherwise you'll get errors such as Could not authenticate to Oracle Database Cloud Backup Module or 403 Forbidden. Set the replication policy and wait at least 10 minutes for synchronization to complete before you retry the installation.

5. Create accounts for your users and assign them appropriate privileges and roles. See Managing User Accounts and Managing User Roles in Managing and Monitoring Oracle Cloud.

   **Note:**
   For Oracle Database Public Cloud Services subscriptions, users must have either the Storage Administrator or Database Backup Administrator role to back up to the cloud.

---

**Frequently Asked Questions for Oracle Database Backup Cloud Service**

For answers to frequently asked questions (FAQs), see the Oracle Database Backup Cloud Service FAQ on My Oracle Support:
Administering Oracle Database Backup Cloud Service

To administer Oracle Database Backup Cloud Service, you’ll install the module needed for cloud backups, configure Recovery Manager (RMAN) settings, and perform other tasks.

Topics
- Typical Workflow for Administering Oracle Database Backup Cloud Service
- Installing the Oracle Database Cloud Backup Module for OCI
- Installing the Oracle Database Cloud Backup Module for OCI Classic
- Configuring Recovery Manager (RMAN) Settings
- Configuring Encryption for Backups
- Configuring Compression for Backups
- Management Interfaces for Cloud Backups
- Storing Backups in Custom Locations
- Configuring Automatic Archival to Oracle Cloud Infrastructure
- Configuring Automatic Archival to Oracle Cloud Infrastructure Classic
- Monitoring Your Storage Capacity

Typical Workflow for Administering Oracle Database Backup Cloud Service

To administer Oracle Database Backup Cloud Service, refer to the following task workflow.

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>More Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Request a trial or purchase a subscription</td>
<td>Sign up for a free trial or purchase a subscription. Then activate your subscription, create accounts for your users, and assign them appropriate privileges and roles.</td>
<td>How to Begin with Oracle Database Backup Cloud Service Subscriptions</td>
</tr>
</tbody>
</table>
Installing the Oracle Database Cloud Backup Module for OCI

To back up to Oracle Cloud Infrastructure, you first need to install the Oracle Database Cloud Backup Module for OCI. You'll download the module from Oracle Technology Network (OTN) and install it on your database server.

Topics

• Before You Begin Installing Oracle Database Cloud Backup Module for OCI
• Supported Databases and Operating Systems
• Parameters to Run the Oracle Database Cloud Backup Module for OCI
• Downloading and Installing the Oracle Database Cloud Backup Module for OCI
Before You Begin Installing Oracle Database Cloud Backup Module for OCI

Before you install the Oracle Database Cloud Backup Module for OCI, make sure you have what you need:

- A supported Oracle Database version and operating system
  See Supported Databases and Operating Systems.

- An Oracle Technology Network (OTN) account or Oracle.com account
  If you don’t have an OTN account, create one by registering at http://www.oracle.com/technetwork/index.html.

- An Oracle Cloud account with access to Oracle Cloud Infrastructure Object Storage
  See Object Storage in the Oracle Cloud Infrastructure Documentation.

- Oracle Cloud Infrastructure API signing keys, tenant OCID, and user OCID
  You may specify a compartment ID. However, if the compartment ID is not specified, the tenant ID is used as the compartment ID.
  See Required Keys and OCIDs.

- JDK 1.7 or later
  You must have JDK 1.7 or later on the system on which you plan to install the Oracle Database Cloud Backup Module for OCI. Use the following command to check your JDK version:
  
  ```
  java -version
  ```

- The required patch if you’re using the Standard Edition of Oracle Database

- Values for the parameters required to run the installer for Oracle Database Cloud Backup Module for OCI
  It’s best to compile this information before you run the installer. See Parameters to Run the Oracle Database Cloud Backup Module for OCI.

**Note:**

If your database server has multiple Oracle homes, the Oracle Database Cloud Backup Module for OCI must be installed into each ORACLE_HOME. Alternatively, you can copy the library file (libopc.so or oraopc.dll, depending on your operating system) to other Oracle home library locations, along with the opcSID.ora configuration file (assuming you’re using the same cloud credentials for backing up all databases in the database server).

Copy and rename the opcSID.ora file for each database instance you are backing up to the cloud, where SID matches the SID for the database instance.
Supported Databases and Operating Systems

You can back up Oracle Database 11g Release 2 (11.2.0.4) and later to Oracle Database Backup Cloud Service.

The following table lists supported database versions and operating systems for operations with Oracle Cloud Infrastructure and Oracle Cloud Infrastructure Classic. It also lists supported Recovery Manager (RMAN) compression and encryption options.

For information about these optimizations, see About Oracle Database Backup Cloud Service.

<table>
<thead>
<tr>
<th>System</th>
<th>Supported Versions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oracle Database*</td>
<td><strong>Enterprise Edition</strong>: 11g Release 2 (11.2.0.4) and later</td>
</tr>
<tr>
<td></td>
<td><strong>Standard Edition (SE, SE1, SE2)</strong>: 11g Release 2 (11.2.0.4) and later</td>
</tr>
<tr>
<td></td>
<td>* Unsupported Oracle Database versions are in deprecated mode. See My Oracle Support Doc ID 1640149.1 at <a href="http://support.oracle.com">http://support.oracle.com</a> for the latest support matrix.</td>
</tr>
<tr>
<td>Operating system (64 bits)</td>
<td>Linux, Solaris x86-64, SPARC, Windows, AIX, HP-UX, zLinux</td>
</tr>
<tr>
<td>RMAN compression</td>
<td>HIGH, MEDIUM, BASIC, LOW</td>
</tr>
<tr>
<td>RMAN encryption</td>
<td><strong>Enterprise Edition</strong>: Password, Transparent Data Encryption (TDE), dual mode.</td>
</tr>
</tbody>
</table>

Parameters to Run the Oracle Database Cloud Backup Module for OCI

You must specify parameters and their values when you run the Oracle Database Cloud Backup Module for OCI installer. It’s best to compile this information before you run the installer.

Parameters include the host name for the Oracle Cloud Infrastructure account and the private key used to sign Oracle Cloud Infrastructure API requests. Parameters can also be displayed by running the following command from the directory that contains the `oci_install.jar` installer file:

```
java -jar oci_install.jar
```

The following example shows what you'll need to provide:

```
java -jar oci_install.jar
-host https://objectstorage.us-phoenix-1.oraclecloud.com
-pvtKeyFile oci_private_key -pubFingerPrint oci_public_fingerprint
-uOCID user_ocid -tOCID tenancy_ocid
-walletDir /wallet_directory -libDir /library_directory
```
The following table lists the required and optional parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Required or Optional</th>
</tr>
</thead>
<tbody>
<tr>
<td>-host</td>
<td>End point of the Oracle Cloud Infrastructure account. For information about finding the Native Oracle Cloud Service Object Storage API endpoints for your account, see the Object Storage FAQs in the Oracle Cloud Infrastructure documentation.</td>
<td>Required</td>
</tr>
<tr>
<td>-pvtKeyFile</td>
<td>File that contains the private key used to authenticate Oracle Cloud Infrastructure API requests. The key file must be in PEM format. See Required Keys and OCIDs in Oracle Cloud Infrastructure Documentation for information about generating API signing keys. This private key is never transmitted outside of the computer where the installer is run.</td>
<td>Required</td>
</tr>
<tr>
<td>-pubFingerPrint</td>
<td>Finger print of the public key paired with the specified private key. The finger print tells Oracle Cloud Infrastructure which private and public key pair is used to authenticate the API requests</td>
<td>Required</td>
</tr>
<tr>
<td>-tOCID</td>
<td>Tenancy OCID for the Oracle Cloud Infrastructure account. See Required Keys and OCIDs in Oracle Cloud Infrastructure Documentation for information about obtaining the tOCID and uOCID.</td>
<td>Required</td>
</tr>
<tr>
<td>-uOCID</td>
<td>User OCID for the Oracle Cloud Infrastructure account.</td>
<td>Required</td>
</tr>
<tr>
<td>-bucket</td>
<td>Name of the bucket in which backups are stored. If this bucket does not exist, then the installer creates it. When this parameter is omitted, a default bucket is automatically created to store backups.</td>
<td>Optional</td>
</tr>
<tr>
<td>-cOCID</td>
<td>Resource compartment ID for the Oracle Cloud Infrastructure account. The default value is the tenancy OCID if not specified.</td>
<td>Optional</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
<td>Required or Optional</td>
</tr>
<tr>
<td>-----------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------------------</td>
</tr>
<tr>
<td>-newRSAKeyPair</td>
<td>Set up a new pair of public and private RSA keys for authentication. If specified, the installer generates a random RSA private and public key pair of 2048 bits and stores them in the specified Oracle wallet directory.</td>
<td>Optional</td>
</tr>
<tr>
<td>-walletDir</td>
<td>Directory in which Oracle Cloud Infrastructure Object Storage credentials are stored. Suggested location on Linux and UNIX systems: ORACLE_HOME/dbs/opc_wallet Suggested location on Windows systems: ORACLE_HOME\database\opc_wallet If the specified wallet directory does not exist (for example, opc_wallet), the installer creates it.</td>
<td>Required</td>
</tr>
<tr>
<td>-libDir</td>
<td>Directory in which the system backup to tape (SBT) library used for backups and restores with Oracle Cloud Infrastructure is stored. If omitted, the library is not downloaded. In most cases, you should specify this parameter and download the library. An exception might be if you’re using the installer to regenerate the wallet and configuration file in an Oracle home directory where the Oracle Database Cloud Backup Module for OCI was previously installed. Suggested location on Linux and UNIX systems: ORACLE_HOME/lib Suggested location on Windows systems: ORACLE_HOME\bin If the specified directory does not exist, you are prompted to create it and then run the installer again.</td>
<td>Required if you want to download the latest module Optional if you just want to update the password after you change it in Oracle Cloud</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
<td>Required or Optional</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>----------------------</td>
</tr>
<tr>
<td>-libPlatform</td>
<td>Operating system for the SBT library used for backups and restores.</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td>In most cases, you don’t need to specify this parameter because the installer automatically determines the correct operating system. Exceptions might be if you see error messages indicating your operating system can’t be identified or if you need to download the library for use on a different system. Supported values for this parameter:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• linux64</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• windows64</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• solaris_sparc64</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• solaris_x64</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• zlinux64</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• hpux_ia64</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• aix_ppc64</td>
<td></td>
</tr>
<tr>
<td></td>
<td>For information about supported operating systems, see Supported Databases and Operating Systems.</td>
<td></td>
</tr>
<tr>
<td>-lib-download-only</td>
<td>Downloads only the SBT library. Use this parameter to update the library without making changes to the configuration file and the wallet.</td>
<td>Optional</td>
</tr>
<tr>
<td>-configFile</td>
<td>Directory in which the Oracle Database Cloud Backup Module for OCI configuration file is stored. If omitted, the configuration file is stored in a default location. Default location on Linux and UNIX systems: ORACLE_HOME/dbs Default location on Windows systems: ORACLE_HOME/database The file name is opcSID.ora, where SID is the system identifier of the Oracle database being backed up to Oracle Cloud Infrastructure Object Storage Service.</td>
<td>Optional</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
<td>Required or Optional</td>
</tr>
<tr>
<td>------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------------------</td>
</tr>
<tr>
<td>-trustedCerts</td>
<td>Comma-separated list of SSL certificates that must be added to the wallet. If the installer is unable to retrieve the certificates required for the SSL connection from local Java truststore, this SSL certificates specified by this parameter are imported. All SSL certificates must be in the PEM format.</td>
<td>Optional</td>
</tr>
<tr>
<td>-import-all-trustcerts</td>
<td>Import all X509 certificates from the Java truststore.</td>
<td>Optional</td>
</tr>
<tr>
<td>-proxyHost</td>
<td>HTTP proxy server host name</td>
<td>Optional</td>
</tr>
<tr>
<td>-proxyPort</td>
<td>HTTP proxy server port number</td>
<td>Optional</td>
</tr>
<tr>
<td>-proxyId</td>
<td>HTTP proxy server user name, if needed.</td>
<td>Optional</td>
</tr>
<tr>
<td>-proxyPass</td>
<td>HTTP proxy server password, if needed.</td>
<td>Optional</td>
</tr>
<tr>
<td>-argFile</td>
<td>Indicates that parameters should be read from the specified file. For example, a file named arguments.txt might contain the following:</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td>-opcID '<a href="mailto:myAccount@myCompany.com">myAccount@myCompany.com</a>' -opcPass 'abc123$' -host <a href="https://objectstorage.us-phoenix-1.oraclecloud.com">https://objectstorage.us-phoenix-1.oraclecloud.com</a> -libDir /home/oracle/OPC/lib -walletDir /home/oracle/OPC/wallet</td>
<td></td>
</tr>
<tr>
<td></td>
<td>For this example, the following command installs the Oracle Database Cloud Backup Module for OCI using the parameters specified in the file:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>java -jar oci_install.jar -argFile arguments.txt</td>
<td></td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
<td>Required or Optional</td>
</tr>
<tr>
<td>------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------------------</td>
</tr>
<tr>
<td>-enableArchiving</td>
<td>Whether backups must be automatically moved from standard Object Storage buckets to Archive Storage. The default value is FALSE. Set this parameter to TRUE to enable automatic archival of backups. Backups are automatically moved to Archive Storage if they meet the criteria set by the object lifecycle policy rule that is associated with the bucket containing the backups. The installer creates an appropriate lifecycle policy rule using the values of the archiveAfterBackup and retainAfterRestore parameters. Do not modify this policy rule. See Using Object Lifecycle Management in the Oracle Cloud Infrastructure Documentation.</td>
<td>Optional</td>
</tr>
<tr>
<td>-archiveAfterBackup</td>
<td>Period of time, in days or years, after which backups are moved from standard Object Storage to Archive Storage. The default is 0 days. This means that the backups are moved to Archive Storage any time between 0 and 24 hours from the time they were created. Examples: -archiveAfterBackup &quot;25 days&quot; -archiveAfterBackup &quot;1 year&quot;</td>
<td>Optional</td>
</tr>
</tbody>
</table>
### Parameter Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Required or Optional</th>
</tr>
</thead>
<tbody>
<tr>
<td>-retainAfterRestore</td>
<td>Period of time, in hours, for which backups that were restored from Archive Storage to standard Object Storage are retained in the Object Storage bucket. The default is 48 hours. Example: -retainAfterRestore &quot;24 hours&quot;</td>
<td>Optional</td>
</tr>
</tbody>
</table>

While restoring using archived backups, the backups must first be recalled from Archive Storage. Recalled backups are retained in Object Storage for the time specified by retainAfterRestore. After the specified time elapses, the backups return to Archive Storage.

### Downloading and Installing the Oracle Database Cloud Backup Module for OCI

Download and install the Oracle Database Cloud Backup Module for OCI on your database server.

First, make sure you’re ready. See Before You Begin Installing Oracle Database Cloud Backup Module for OCI.

To download and install the Oracle Database Cloud Backup Module for OCI:

1. Download the Oracle Database Cloud Backup Module for OCI from Oracle Technology Network (OTN):
   
   
   Accept the license agreement, click All Supported Platforms, and provide your OTN user name and password when prompted. Then download the ZIP file that contains the installer (opc_installer.zip) to your system.

2. Extract the contents of the zip file.
   
   The file contains two directories, oci_installer and opc_installer, and a README file.

3. (Optional) To configure automatic movement of backups from standard Object Storage to Archive Storage, authorize the Object Storage service to move backups to Archive Storage. See Service Permissions in the Required IAM Policies section of the Oracle Cloud Infrastructure documentation.

4. Run the installer, oci_install.jar, from the oci_installer directory. Provide the required parameters in one line, with each parameter preceded by a hyphen and
followed by its value. For information about required parameters, see Parameters to Run the Oracle Database Cloud Backup Module for OCI.

Example 2-1 Installing the Oracle Database Cloud Backup Module for OCI

The following is an example run of the installer. This example shows how the installer automatically downloads the Oracle Database Cloud Backup Module for OCI for your operating system, creates a wallet that contains Oracle Database Backup Cloud Service identifiers and credentials, creates the backup module configuration file, and downloads the library necessary for backups and restores to Oracle Cloud Infrastructure.

% java -jar oci_install.jar -host https://objectstorage.us-phoenix-1.oraclecloud.com
-pvtKeyFile /oracle/dbs/oci_wallet/oci_pvt
-uOCID
ocid1.user.oc1..aaaaaaaasd754pijuwheaq67t7tninefkn7z7aibttusj7jqac5lp7w37va
-tOCID
ocid1.tenancy.oc1..aaaaaaavjhwf4c7q2ozzyduh7njrft58i6ts3ryjkc7v83w7q4wdr2ka
-walletDir /oracle/dbs/oci_wallet
-libDir /oracle/lib
-bucket db_backups
Oracle Database Cloud Backup Module Install Tool, build 2018-12-11
Oracle Database Cloud Backup Module credentials are valid.
Backups would be sent to bucket db_backups.
Oracle Database Cloud Backup Module wallet created in directory /oracle/dbs/
oci_wallet.
Oracle Database Cloud Backup Module initialization file /oracle/dbs/opcb18test.ora
 created.
Downloading Oracle Database Cloud Backup Module Software Library from file
opc_linux64.zip.
Download complete.

Example 2-2 Enabling Automatic Archival of Backups When Installing the Oracle Database Cloud Backup Module for OCI

This example installs the Oracle Database Cloud Backup Module for OCI and creates a standard bucket named backup_archival_60, with archiving enabled. Backups stored in this bucket are automatically moved from standard Object Storage to Archive Storage 60 days after they are created. During a restore operation, backups recalled from Archive Storage are retained in the Object Storage bucket for 72 hours. An object lifecycle policy is created and associated with the bucket backup_archival_60. The information specified in the -archiveAfterBackup and -retainAfterRestore parameters are stored in this object lifecycle policy.

Before you run the installer, ensure that you authorize the Object Storage service to move backups to Archive Storage, as described in Step 3.

% java -jar oci_install.jar
-host https://objectstorage.us-phoenix-1.oraclecloud.com
-pvtKeyFile /home/database/oci_wallet/oci_pvt
-tOCID
ocid1.tenancy.oc1..aaaaaaavjhwf4c7q2ozzyduh7njrft58i6ts3ryjkc7v83w7q4wdr2ka
-c8le
-uOCID
ocid1.user.oc1..aaaaaaarg468pilujhpa45t1mjesurg5z7sapude55jqax47pm2cx7lv
a
-cOCID
Oracle Database Cloud Backup Module Install Tool, build 19.3.0.0.0DBBKPCSBP_2019-10-09
Oracle Database Cloud Backup Module credentials are valid.
Backups would be sent to bucket backup_archival_60.
Oracle Database Cloud Backup Module wallet created in directory /database/dbs/oci_wallet.
Oracle Database Cloud Backup Module initialization file /home/database/oci_config.ora created.
Downloading Oracle Database Cloud Backup Module Software Library from Oracle Cloud Infrastructure.
Download complete.

Files Created when Oracle Database Cloud Backup Module for OCI is Installed

After you run the installer for the Oracle Database Cloud Backup Module for OCI, make sure the required files are on your system.

The following files are created when you install the backup module and they are used to perform cloud backups and restores. For information about the parameters mentioned, see Parameters to Run the Oracle Database Cloud Backup Module for OCI.

<table>
<thead>
<tr>
<th>File</th>
<th>Location</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>libopc.so on Linux and UNIX systems</td>
<td>As specified for the -libDir parameter when you run the installer for the Oracle Database Cloud Backup Module for OCI. Example location: ORACLE_HOME/lib</td>
<td>Operating system-specific SBT library that enables cloud backups and restores with the Oracle Cloud Infrastructure.</td>
</tr>
<tr>
<td>oraopc.dll on Windows systems</td>
<td></td>
<td></td>
</tr>
<tr>
<td>opcSID.ora</td>
<td>As specified for the -configFile parameter when you run the installer for the Oracle Database Cloud Backup Module for OCI. Default location on Linux and UNIX systems: ORACLE_HOME/dbs Default location on Windows systems: ORACLE_HOME\database</td>
<td>Configuration file that contains the Oracle Cloud Infrastructure Object Storage bucket URL and credential wallet location, where SID is the system identifier of the Oracle database being backed up to Oracle Cloud Infrastructure.</td>
</tr>
</tbody>
</table>
### Installing the Oracle Database Cloud Backup Module for OCI Classic

To back up to Oracle Cloud Infrastructure Classic, you first need to install the Oracle Database Cloud Backup Module for OCI Classic. You'll download the module from Oracle Technology Network (OTN) and install it on your database server.

**Topics**

- **Before You Begin Installing Oracle Database Cloud Backup Module for OCI Classic**
- **Supported Databases and Operating Systems**
- **Parameters Used to Run the Oracle Database Cloud Backup Module for OCI Classic Installer**
- **Downloading and Installing the Oracle Database Cloud Backup Module for OCI Classic**
- **Files Created When the Oracle Database Cloud Backup Module for OCI Classic is Installed**

### Before You Begin Installing Oracle Database Cloud Backup Module for OCI Classic

Before you install the Oracle Database Cloud Backup Module for OCI Classic, make sure you have what you need:

- A supported Oracle Database version and operating system
  
  See [Supported Databases and Operating Systems](#).

- An Oracle Technology Network (OTN) account or Oracle.com account
  
  If you don't have an OTN account, create one by registering at [http://www.oracle.com/technetwork/index.html](http://www.oracle.com/technetwork/index.html).

- An Oracle Database Backup Cloud Service account and storage capacity
  
  See [How to Begin with Oracle Database Backup Cloud Service Subscriptions](#).

- JDK 1.7 or later

### Files

<table>
<thead>
<tr>
<th>File</th>
<th>Location</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>cwallet.sso</td>
<td>As specified for the --walletDir parameter when you run the Oracle Database Cloud Backup Module for OCI installer. Example location: ORACLE_HOME/dbs/opc_wallet</td>
<td>Oracle wallet file that securely stores Oracle Cloud Infrastructure Object Storage credentials. This file is used during Recovery Manager (RMAN) backup and restore operations and is stored in the Oracle Cloud Infrastructure Object Storage wallet directory (for example, opc_wallet).</td>
</tr>
</tbody>
</table>
You must have JDK 1.7 or later on the system on which you plan to install the Oracle Database Cloud Backup Module for OCI Classic. Use the following command to check your JDK version:

```java
java -version
```

- The required patch if you're using the Standard Edition of Oracle Database
- See My Oracle Support Doc ID 1640149.1 at [http://support.oracle.com](http://support.oracle.com).
- Values for the parameters required to run the Oracle Database Cloud Backup Module for OCI Classic installer
- It's best to compile this information before you run the installer. See Parameters Used to Run the Oracle Database Cloud Backup Module for OCI Classic Installer.

---

**Note:**

If your database server has multiple Oracle homes, the Oracle Database Cloud Backup Module for OCI Classic must be installed into each `ORACLE_HOME`. Alternatively, you can copy the library file (`libopc.so` or `oraopc.dll`, depending on your operating system) to other Oracle home library locations, along with the `opcSID.ora` configuration file (assuming you're using the same cloud credentials for backing up all databases in the database server).

Copy and rename the `opcSID.ora` file for each database instance you are backing up to the cloud, where `SID` matches the SID for the database instance.

---

### Parameters Used to Run the Oracle Database Cloud Backup Module for OCI Classic Installer

You'll need to specify parameters and their values when you run the Oracle Database Cloud Backup Module for OCI Classic installer. Parameters include host (REST endpoint) and account credentials. It's best to compile this information before you run the installer.

The following example shows what you'll need to provide:

```java
java -jar opc_install.jar
-host https://foo.storage.oraclecloud.com/v1/Storage-myIdentity3
-opcid 'myAccount@myCompany.com' -opcpass 'opc_password'
-walletDir /walletDirectory -libDir /libraryDirectory
```

The following table lists required parameters. Optional parameters are also listed.

Parameters can also be displayed by running the following command from the directory that contains the `opc_install.jar` installer file:

```java
java -jar opc_install.jar
```
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Required or Optional</th>
</tr>
</thead>
<tbody>
<tr>
<td>-host</td>
<td>REST endpoint for your service as listed on the service details page. For information about finding the URL for your account, see About REST URLs for Oracle Storage Cloud Service Resources in Using Oracle Storage Cloud Service. For example: -host <a href="https://abc.storage.oraclecloud.com/v1/hr-abc">https://abc.storage.oraclecloud.com/v1/hr-abc</a></td>
<td>Required</td>
</tr>
<tr>
<td>-opcId</td>
<td>User name for your Oracle Database Backup Cloud Service account. Enclose the user name in single quotes, for example '<a href="mailto:myAccount@myCompany.com">myAccount@myCompany.com</a>'. On Windows systems, use double quotes if the user name contains special characters.</td>
<td>Required</td>
</tr>
<tr>
<td>-opcPass</td>
<td>Password for the Oracle Database Backup Cloud Service account specified by -opcId. Enclose the password in single quotes, for example 'opc_password'. On Windows systems, use double quotes if the password contains special characters.</td>
<td>Required</td>
</tr>
<tr>
<td>-walletDir</td>
<td>Directory in which Oracle Database Backup Cloud Service credentials are stored. Suggested location on Linux and UNIX systems: ORACLE_HOME/dbs/opc_wallet Suggested location on Windows systems: ORACLE_HOME\database\opc_wallet If the specified wallet directory does not exist (for example, opc_wallet), the installer creates it.</td>
<td>Required</td>
</tr>
<tr>
<td>-libDir</td>
<td>Directory in which the system backup to tape (SBT) library used for backups and restores is stored. This parameter is required if you want to download the latest module. Optional if you just want to update the password after you change it in Oracle Cloud. If omitted, the library is not downloaded. In most cases, you should specify this parameter and download the library. An exception might be if you're using the installer to regenerate the wallet and configuration file in an Oracle home directory where the Oracle Database Cloud Backup Module for OCI Classic was previously installed. Suggested location on Linux and UNIX systems: ORACLE_HOME/lib Suggested location on Windows systems: ORACLE_HOME\bin If the specified directory does not exist, you are prompted to create it and then run the installer again.</td>
<td>Required if you want to download the latest module Optional if you just want to update the password after you change it in Oracle Cloud</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
<td>Required or Optional</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
<td>---------------------</td>
</tr>
<tr>
<td><code>-libPlatform</code></td>
<td>Operating system for the SBT library used for backups and restores. In most cases, you don’t need to specify this parameter because the installer automatically determines the correct operating system. Exceptions might be if you see error messages indicating your operating system can’t be identified or if you need to download the library for use on a different system. Supported values for this parameter: • <code>linux64</code> • <code>windows64</code> • <code>solaris_sparc64</code> • <code>solaris_x64</code> • <code>zlinux64</code> • <code>hpux_ia64</code> • <code>aix_ppc64</code> For information about supported operating systems, see Supported Databases and Operating Systems.</td>
<td>Optional</td>
</tr>
<tr>
<td><code>-container</code></td>
<td>Custom container created by you, separate from Oracle Database Backup Cloud Service, to store backups. If omitted, backups are stored in the default container that’s created when the backup module is installed. See Storing Backups in Custom Locations. <strong>Note:</strong> Containers that are used by Recovery Manager (RMAN) cannot have server-side encryption enabled. Because RMAN backups are already encrypted at the client side, server-side encryption is not required.</td>
<td>Optional</td>
</tr>
<tr>
<td><code>-containerClass</code></td>
<td>Storage class of the custom container. The valid values for this parameter are: • <code>Standard</code>: Represents Standard storage container. • <code>Tiering</code>: Represents a Standard storage container whose Lifecycle Tiering Policy is set. This option creates a container for which automatic archive is enabled. The tiering policy controls the frequency at which objects stored in this container are archived. The Oracle Database Cloud Backup Module for OCI Classic sets default parameters for the tiering policy. The default tiering policy excludes XML files and moves backups to archive storage immediately. If this parameter is omitted, then the default is either <code>Standard</code> or the storage class of the container specified using <code>-container</code>, if the container exists.</td>
<td>Optional</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
<td>Required or Optional</td>
</tr>
<tr>
<td>---------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------------------</td>
</tr>
<tr>
<td>-containerLTP</td>
<td>Name of Lifecycle Tiering Policy (LTP) file. This file is a JSON document that specifies the time after which objects in the storage container will be moved to the archive tier and type of objects which can be excluded from being archived. To create archival backups, specify the name of the LTP file that defines the archival policy for the storage container by using the <code>-containerLTP</code> parameter. You can optionally set <code>-containerClass</code> to <code>Tiering</code>. <strong>Note:</strong> The Lifecycle Tiering Policy file must exclude XML files. If this is not done, an error is displayed both when installing and using the Oracle Database Cloud Backup Module for OCI Classic. The exclusions field of the policy must be exactly like the one shown in Example 2-5.</td>
<td>Optional</td>
</tr>
<tr>
<td>-configFile</td>
<td>Directory in which the Oracle Database Cloud Backup Module for OCI Classic configuration file is stored. If omitted, the configuration file is stored in a default location. Default location on Linux and UNIX systems: <code>ORACLE_HOME/dbs</code> Default location on Windows systems: <code>ORACLE_HOME\database</code> The file name is <code>opcSID.ora</code>, where <code>SID</code> is the system identifier of the Oracle database being backed up to Oracle Database Backup Cloud Service.</td>
<td>Optional</td>
</tr>
<tr>
<td>-proxyHost</td>
<td>HTTP proxy server host name</td>
<td>Optional</td>
</tr>
<tr>
<td>-proxyPort</td>
<td>HTTP proxy server port number</td>
<td>Optional</td>
</tr>
<tr>
<td>-proxyId</td>
<td>HTTP proxy server user name, if needed</td>
<td>Optional</td>
</tr>
<tr>
<td>-proxyPass</td>
<td>HTTP proxy server password, if needed</td>
<td>Optional</td>
</tr>
</tbody>
</table>
| -argFile      | Indicates that parameters should be read from the specified file. For example, a file named `arguments.txt` might contain the following:  

```
-opcID 'myAccount@myCompany.com'
-opcPass 'abc123$'
-host https://
foo.storage.oraclecloud.com/v1/
Storage-myIdentity3
-libDir /home/oracle/OPC/lib
-walletDir /home/oracle/OPC/wallet
```

For this example, the following command installs the Oracle Database Backup Module for OCI Classic using the parameters specified in the file:

```
java -jar opc_install.jar -argFile arguments.txt
```
Downloading and Installing the Oracle Database Cloud Backup Module for OCI Classic

Download and install the Oracle Database Cloud Backup Module for OCI Classic on your database server.

First, make sure you're ready. See Before You Begin Installing Oracle Database Cloud Backup Module for OCI Classic.

To download and install the Oracle Database Cloud Backup Module for OCI Classic:

1. Download the Oracle Database Cloud Backup Module for OCI Classic from Oracle Technology Network (OTN):


   Accept the license agreement, click All Supported Platforms, and provide your OTN user name and password when prompted. Then download the ZIP file that contains the installer (opc_installer.zip) to your system.

2. Extract the contents of the zip file.

   The file contains two directories, oci_installer and opc_installer, and a README file.

3. Run the installer, opc_install.jar, from the opc_installer directory. Provide the required parameters in one line, with each parameter preceded by a hyphen and followed by its value. For information about required parameters, see Parameters Used to Run the Oracle Database Cloud Backup Module for OCI Classic Installer.

Example 2-3   Installing the Oracle Database Cloud Backup Module for OCI Classic

This example shows how the installer automatically downloads the Oracle Database Cloud Backup Module for OCI Classic for your operating system, creates a wallet that contains Oracle Database Cloud Backup Service identifiers and credentials, creates the Oracle Database Cloud Backup Module for OCI Classic configuration file, and downloads the library necessary for cloud backups and restores.

```
java -jar opc_install.jar -host https://myDomain.storage.oraclecloud.com/v1/
   myService-myDomain
   -opcId 'myAccount@myCompany.com' -opcPass 'opc_pswd1'
   -walletDir /home/oracle/OPC/wallet -libDir /home/oracle/OPC/lib
```

Oracle Database Cloud Backup Module Install Tool, build 2017-08-15
Oracle Database Cloud Backup Module credentials are valid.
Oracle Database Cloud Backup Module wallet created in directory /home/oracle/OPC/wallet.
Oracle Database Cloud Backup Module initialization file /orclhome/dbs/opcmySID.ora created.
Downloading Oracle Database Cloud Backup Module Software Library from file opc_linux64.zip.
Download complete.
Example 2-4  Creating a Tiering Container When Installing the Oracle Database Cloud Backup Module for OCI Classic

This example installs the Oracle Database Cloud Backup Module for OCI Classic and creates a container named `archive_container` for which automatic archiving is enabled. To create a container with automatic archiving, you must specify `Tiering` for the `containerClass`. A default Lifecycle Tiering Policy is associated with this container and the values specified by the tiering policy control when backups stored in this container are moved to archive storage.

```
% java -jar opc_install.jar -host https://myDomain.storage.oraclecloud.com/v1/myService-myDomain/
   -opcId 'myAccount@myCompany.com' -opcPass 'opc_pswd1'
   -walletDir /home/oracle/opc/opc_wallet
   -libDir /home/oracle/lib
   -containerClass Tiering -container archive_container
```

Oracle Database Cloud Backup Module Install Tool, build MAIN_2017-09-12
Oracle Database Cloud Backup Module credentials are valid.
Backups would be sent to container `archive_container`.
Oracle Database Cloud Backup Module wallet created in directory `/home/oracle/opc/opc_wallet`.
Oracle Database Cloud Backup Module initialization file `/orclhome/dbs/opcdb18c.ora` created.
Downloading Oracle Database Cloud Backup Module Software Library from file `opc_linux64.zip`.
Download complete.

Example 2-5  JSON Document for Lifecycle Tiering Policy File

The following example shows a JSON document that contains the information required to define a Lifecycle Tiering Policy for an archive container. The Lifecycle Tiering Policy set using this JSON document excludes all XML files from the backup and moves backups to the Archive tier after 7 days.

```
{
  "archiveAfter":{
    "timeUnit":"DAYS",
    "time":7
  },
  "exclusions":{
    "exclusionType":"REGEX",
    "exclusionFilter":"\.xml"
  }
}
```

Note: A value greater than 0 for `archiveAfter` is only supported in limited data centers.
You can run the installer and install the Oracle Database Cloud Backup Module for OCI Classic as many times as you like. Periodically perform the installation procedure to get the latest RMAN SBT library module, and also to update the password after you change it in Oracle Cloud.

Files Created When the Oracle Database Cloud Backup Module for OCI Classic is Installed

After you run the installer for the Oracle Database Cloud Backup Module for OCI Classic, make sure the required files are on your system.

The following files are created when you install the Oracle Database Cloud Backup Module for OCI Classic and are used by Oracle Database Backup Cloud Service to perform cloud backups and restores. For information about the parameters mentioned, see Parameters Used to Run the Oracle Database Cloud Backup Module for OCI Classic Installer.

<table>
<thead>
<tr>
<th>File</th>
<th>Location</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>libopc.so on Linux and UNIX systems</td>
<td>As specified for the -libDir parameter when you run the Oracle Database Cloud Backup Module for OCI Classic installer. Example location: ORACLE_HOME/lib</td>
<td>Operating system-specific SBT library that enables cloud backups and restores.</td>
</tr>
<tr>
<td>oraopc.dll on Windows systems</td>
<td></td>
<td></td>
</tr>
<tr>
<td>opcSID ora</td>
<td>As specified for the -configFile parameter when you run the Oracle Database Cloud Backup Module for OCI Classic installer. Default location on Linux and UNIX systems: ORACLE_HOME/dbs Default location on Windows systems: ORACLE_HOME\database</td>
<td>Configuration file that contains the Oracle Database Backup Cloud Service container URL and credential wallet location, where SID is the system identifier of the Oracle database being backed up to Oracle Database Backup Cloud Service. <strong>Note:</strong> Containers that are used by Recovery Manager (RMAN) cannot have server-side encryption enabled. Because RMAN backups are already encrypted at the client side, server-side encryption is not required.</td>
</tr>
</tbody>
</table>
### Configuring Recovery Manager (RMAN) Settings

After you install the Oracle Database Cloud Backup Module for OCI or the Oracle Database Cloud Backup Module for OCI Classic, configure Recovery Manager (RMAN) to use Oracle Database Backup Cloud Service as the backup destination.

You’ll use the `CONFIGURE` command to create or change a persistent configuration affecting RMAN backup, restore, and maintenance. The location to which backups are stored is determined by the configuration that is currently in use. For example, if the current configuration is to Oracle Cloud using the Oracle Database Cloud Backup Module for OCI, then this location is used for backup and restore operations. To back up to a different location, for example Oracle Cloud Infrastructure Classic, you just configure a channel that corresponds to Oracle Database Cloud Backup Module for OCI Classic.

For more information about the command, see `CONFIGURE` in *Oracle Database Backup and Recovery Reference*.

#### Configuring Autobackup

As a best practice, you should also configure RMAN to automatically back up the database control file and server parameter file. With a control file autobackup, RMAN can recover the database even if the current control file, recovery catalog, and server parameter file are inaccessible.

The autobackup feature is disabled by default. To enable autobackup, use the following command:

```
RMAN> CONFIGURE CONTROLFILE AUTOBACKUP ON;
```

For information about configuring automatic archive for backups, see Configuring Automatic Archival to Oracle Cloud Infrastructure Classic.

For information about autobackups, see About RMAN Control File and Server Parameter File Autobackups in *Oracle Database Backup and Recovery User’s Guide*.

For information about RMAN commands, see About RMAN Commands in *Oracle Database Backup and Recovery Reference*.

#### Example 2-6 Configuring RMAN to Back Up to Oracle Cloud Infrastructure

On Linux and UNIX systems, the following command configures an RMAN channel that uses the Oracle Database Cloud Backup Module for OCI SBT library for backup and restore operations to Oracle Cloud Infrastructure:

```sql
RMAN> CONFIGURE CHANNEL ‘oci’ IDENTIFIED BY ‘oci_password’ LOCATION ‘oci://oci/your_bucket/backup’;
```
RMAN> CONFIGURE CHANNEL DEVICE TYPE sbt
PARMS='SBT_LIBRARY=location-of-the-SBT-library-OCI-Backup-Module-for-OCI,
SBT_PARMS=(OPC_PFILE=location-of-the-configuration file)';

For example:
RMAN> CONFIGURE CHANNEL DEVICE TYPE sbt
PARMS='SBT_LIBRARY=/orclhome/lib/libopc.so,
SBT_PARMS=(OPC_PFILE=/orclhome/dbs/opcora12.ora)';

On Windows systems, you'll need to specify the ENV parameter. For example:
RMAN> CONFIGURE CHANNEL DEVICE TYPE sbt
PARMS='SBT_LIBRARY=C:\tmp\oraopc.dll,
ENV=(OPC_PFILE=C:\tmp\opcora12.ora)';

**Example 2-7 Configuring RMAN to Back Up to Oracle Cloud Infrastructure Classic**

On Linux and UNIX systems, the following command configures an RMAN channel that uses the Oracle Database Cloud Backup Module for OCI Classic SBT library and configuration file for backup to the cloud:

RMAN> CONFIGURE CHANNEL DEVICE TYPE sbt
PARMS='SBT_LIBRARY=location-of-the-SBT-library-for-Database-Cloud-Backup-Module-for-OCIClassic,
SBT_PARMS=(OPC_PFILE=location-of-the-configuration file)';

For example:
RMAN> CONFIGURE CHANNEL DEVICE TYPE sbt
PARMS='SBT_LIBRARY=/orclhome/lib/libopc.so,
SBT_PARMS=(OPC_PFILE=/orclhome/dbs/opct1.ora)';

**Note:**
For Oracle Database 10g Release 2 (10.2), specify the ENV parameter instead of the SBT_PARMS parameter shown in the previous example. For example:

RMAN> CONFIGURE CHANNEL DEVICE TYPE sbt
PARMS='SBT_LIBRARY=/orclhome/lib/libopc.so,
ENV=(OPC_PFILE=/orclhome/dbs/opct1.ora)';

On Windows systems, you'll need to specify the ENV parameter. For example:
RMAN> CONFIGURE CHANNEL DEVICE TYPE sbt
PARMS='SBT_LIBRARY=C:\tmp\oraopc.dll,
ENV=(OPC_PFILE=C:\tmp\opct1.ora)';

You can configure as many RMAN channels as you want. Once the RMAN configuration is done, you can perform cloud backups and restores using any of the RMAN commands you usually use.

Note:
In a Windows environment, install the oraopc.dll library file in the ORACLE_HOME/bin directory, or pass ORACLE_HOME as a parameter to the channel by using sbt PARMS.

Use the SHOW ALL command to confirm you've configured RMAN to use Oracle Database Backup Cloud Service as the backup destination:

RMAN> SHOW ALL;

You'll see an entry similar to this in your list of settings:

CONFIGURE CHANNEL DEVICE TYPE 'SBT_TAPE' PARMS 'SBT_LIBRARY=/orclhome/lib/libopc.so, SBT_PARMS=(OPC_PFILE=/orclhome/dbs/opct1.ora)';

Configuring Encryption for Backups

Backups must be encrypted before they can be sent to Oracle Database Backup Cloud Service. You'll specify encryption when you perform a backup.

If a backup is not encrypted, you'll get an error message similar to the one shown below when you try to back up to the service:

RMAN-03009: failure of backup command on ORA_SBT_TAPE_1 channel at 08/15/2014 14:00:43
ORA-27030: skgfwrt: sbtwrite2 returned error
ORA-19511: non RMAN, but media manager or vendor specific failure, error text: KBHS-01602: backup piece 14p0jso8_1_1 is not encrypted

Recovery Manager (RMAN) encrypted backups are securely created, transmitted, and stored in the cloud. Use one of the following RMAN encryption modes to encrypt backups:

• Password encryption
• Transparent Data Encryption (TDE)
• Dual-mode encryption (combination of password and TDE)

For information about encryption methodologies and choosing an encryption algorithm, see Configuring Backup Encryption in Oracle Database Backup and Recovery User's Guide.

Configuring Compression for Backups

You can optionally use compression when backing up Oracle databases to Oracle Database Backup Cloud Service. Compression conserves bandwidth by reducing the
size of your backups before they’re sent to the cloud. You’ll specify compression when you perform a backup.

Recovery Manager (RMAN) supports binary compression using one of the following compression levels: HIGH, MEDIUM, BASIC, and LOW. The recommended level for cloud backups is MEDIUM.

For example, the following RMAN commands configure compression using the MEDIUM algorithm:

```
RMAN> CONFIGURE COMPRESSION ALGORITHM 'MEDIUM';
RMAN> CONFIGURE DEVICE TYPE sbt BACKUP TYPE TO COMPRESSED BACKUPSET;
```

Backups must be in the form of backup sets, not image copies. For information about configuring compression for backups, see Configuring Compression Options in Oracle Database Backup and Recovery User’s Guide.

Management Interfaces for Cloud Backups

You can use any of the following options to manage cloud backup operations.

- **RMAN interface**
  Use the RMAN command-line interface to execute familiar commands and perform backups on demand. You can also create automated backup jobs using the cron utility.

- **Oracle Enterprise Manager Cloud Control 13c**
  Use Oracle Enterprise Manager Cloud Control 13c to configure the backup module and perform backup and recovery operations.

- **Third-party tools**
  Use third-party tools such as CloudBerry Lab’s cloud backup solution. See [https://www.cloudberrylab.com/backup.aspx](https://www.cloudberrylab.com/backup.aspx).

Storing Backups in Custom Locations

A default location is created when you install the Oracle Database Cloud Backup Module for OCI or Oracle Database Cloud Backup Module for OCI Classic and backups are stored as objects in this location. You can also store backups in custom locations you’ve created yourself.

With the Oracle Database Cloud Backup Module for OCI, a default bucket is created. With the Oracle Database Cloud Backup Module for OCI Classic, a default storage container is created.

Custom containers and custom buckets can be created using REST calls or third-party tools such as CloudBerry Explorer (see How to Use CloudBerry Explorer with Oracle Cloud Storage from CloudBerry Lab).

To create containers using the REST API, see the tutorial Oracle Storage Cloud Service: Creating Containers Using the REST API. For related Oracle Storage Cloud Service documentation, see Creating Containers and Authenticating Access to Oracle Storage Cloud Service in Using Oracle Storage Cloud Service.

To create buckets using the REST API or Console, see Creating Buckets.
Note:

If you're using Oracle Database Cloud Service or Oracle Database Exadata Cloud Service and want to automatically store backups in cloud storage, you need to create an Oracle Storage Cloud Service container before you create your database deployment. For information about backing up your deployment to the cloud, see Backing Up and Restoring Databases on Database Cloud Service in Using Oracle Database Cloud Service or Backing Up and Restoring Databases on Exadata Cloud Service in Using Oracle Database Exadata Cloud Service.

Note:

Containers that are used by Recovery Manager (RMAN) cannot have server-side encryption enabled. Because RMAN backups are already encrypted at the client side, server-side encryption is not required.

Example 2-8 Using Custom Buckets with Oracle Cloud Infrastructure

You can specify that backups must be stored in custom containers either while installing the Oracle Database Cloud Backup Module for OCI or after the installation.

- While running the Oracle Database Cloud Backup Module for OCI installer, include the -bucket parameter and the custom bucket name.

  For example:

  `-bucket SALES_DB`

  This automatically adds the OPC_CONTAINER parameter to the opcSID.ora configuration file so the custom bucket is used for backups, where SID is the system identifier of the Oracle database being backed up to Oracle Database Backup Cloud Service.

- To specify a custom container after you've installed the Oracle Database Cloud Backup Module for OCI, add the OPC_CONTAINER parameter and the bucket name to opcSID.ora.

  For example:

  `OPC_CONTAINER=SALES_DB`

Example 2-9 Using Custom Containers with Oracle Cloud Infrastructure Classic

Specify that backups must be stored in a custom container either while installing the Oracle Database Cloud Backup Module for OCI Classic or after the installation.

- While running the Oracle Database Cloud Backup Module for OCI Classic installer, include the -container parameter and the custom container name.

  For example:

  `-container PAYROLL_DB`
This automatically adds the OPC_CONTAINER parameter to the opcSID.ora configuration file so the custom container is used for backups, where SID is the system identifier of the Oracle database being backed up to Oracle Database Backup Cloud Service.

- To specify a custom container after you’ve installed the Oracle Database Cloud Backup Module for OCI Classic, add the OPC_CONTAINER parameter and the container name to opcSID.ora.

For example:

OPC_CONTAINER=PAYROLL_DB

For information about parameters used by the installer, see Parameters Used to Run the Oracle Database Cloud Backup Module for OCI Classic Installer.

For information about the opcSID.ora configuration file, see Files Created When the Oracle Database Cloud Backup Module for OCI Classic is Installed.

For information about the opcSID.ora configuration file, see Files Created when Oracle Database Cloud Backup Module for OCI is Installed.

Configuring Automatic Archival to Oracle Cloud Infrastructure

You can move backups that are rarely accessed, but must be retained for long periods, to Archive Storage. Archive Storage is more cost effective than Object Storage for preserving cold data.

You can either create a new bucket or use an existing bucket to store backups that must be automatically moved to Archive Storage.

To configure automatic archival of backups to Oracle Cloud Infrastructure Archive Storage:

1. Authorize Object Storage service to move backups to Archive Storage. See Service Permissions in Using Object Lifecycle Management of the Oracle Cloud Infrastructure Documentation.

2. To use an existing bucket, ensure that automatic archival is enabled for the bucket.

   a. Check if automatic archival is enabled by viewing the bucket details. See Managing Buckets in the Oracle Cloud Infrastructure Documentation.

   b. If automatic archival is not enabled, run the installer with the –enableArchiving parameter to enable archiving for the bucket.

   The command to run the installer is similar to the one in Downloading and Installing the Oracle Database Cloud Backup Module for OCI. The –bucket parameter must specify the name of the existing bucket. The default values are used if the –archiveAfterBackup and –retainAfterRestore parameters are not specified.

   An archiving rule is applied to all the existing objects in the bucket. For example, if you apply a lifecycle policy that archives after two weeks to an existing bucket containing objects, all the objects older than two weeks will be archived.
3. To create a new bucket, run the installer with the `-bucket` and `-enableArchiving` parameters.

   See [Downloading and Installing the Oracle Database Cloud Backup Module for OCI](#) for an example.

4. Configure an RMAN channel that corresponds to the Oracle Database Cloud Backup Module for OCI.

   The following command configures an RMAN channel that uses Oracle Cloud Infrastructure as the backup destination:

   ```
   RMAN> CONFIGURE CHANNEL DEVICE TYPE 'SBT_TAPE' PARMS 'SBT_LIBRARY=/home/database/oracle/lib/libopc.so,SBT_PARMS=(OPC_PFILE=/home/database/oracle/oci_config.ora)';
   ```

---

**Configuring Automatic Archival to Oracle Cloud Infrastructure Classic**

Infrequently-used backups can be moved from standard storage and archived after a specified number of days. This frees up space on the standard storage for new backups.

To archive backups, you must store them in a standard container that is associated with a Lifecycle Tiering Policy (LTP). The LTP is a container policy that defines the type of tiering that is associated with the standard container. After the number of days specified by the LTP elapses, the backups stored in the standard container are automatically archived. You can explicitly exclude specific objects from being archived automatically.

To configure automatic archive of backups to Oracle Cloud Infrastructure Classic:

1. Use one of the following techniques, when installing the Oracle Database Cloud Backup Module for OCI Classic, to specify the container to which backups must be archived:

   - Create a standard container that is associated with an LTP

     Specify the name that must be used for the new standard container by using the `-container` parameter. Set the `-containerClass` parameter to Tiering. To specify a user-defined LTP, use the `-containerLTP` parameter. If you omit this parameter, the default LTP is associated with the new container.

     See [Downloading and Installing the Oracle Database Cloud Backup Module for OCI Classic](#) for an example:

     ```
     -container PAYROLL_ARC -containerClass Tiering
     ```

     The standard container with the specified name is created and a default LTP is assigned to it. All backups, except XML objects, are archived when the number of days specified by the LTP elapses. This automatically adds the `OPC_CONTAINER` and `OPC_CONTAINER_CLASS` parameters to the opcSID.ora file so that these settings are used for backups.
• Specify only the container class
  Set `-containerClass` to `Tiering`.
  The `OPC_CONTAINER_CLASS` parameter is set to `Tiering` in the `opcSID.ora` configuration file. The Oracle Database Cloud Backup Module for OCI Classic installer attempts to find an existing standard container that is associated with an LTP. If no such container is found, a new standard container with the default LTP is created. The naming convention used for the new container is `oracle-data-account_name-index`.

• Use an existing standard container that is associated with an LTP
  Include the `-container` parameter with the name of an existing standard container that is associated with an LTP.
  For example:

  `-container PAYROLL_ARC`

  This automatically adds the `OPC_CONTAINER` parameter to the `opcSID.ora` configuration file so that the specified container is used to store backups.

2. Configure an RMAN channel that corresponds to the Oracle Database Cloud Backup Module for OCI Classic.

   The following command, on Linux, configures an RMAN channel that uses Oracle Cloud Infrastructure Classic as a destination:

   ```
   RMAN> CONFIGURE CHANNEL DEVICE TYPE sbt
   PARMS='SBT_LIBRARY=/orclhome/lib/libopc.so,'
   ENV=(OPC_PFILE=/orclhome/dbs/opct1.ora);'
   ```

Monitoring Your Storage Capacity

When you subscribe to Oracle Database Backup Cloud Service you purchase the amount of storage capacity you want for your backups. If you reach your storage capacity limit and try to back up your database, your backup will fail.

You can quickly increase the limit by purchasing more capacity on demand. Once you buy more capacity, you can continue doing backups. You can also free up space by using RMAN to delete obsolete backups.

You can monitor how much storage capacity you’ve used by viewing detailed metrics about your usage. If your backups are stored in Object Storage Classic, use the Infrastructure Classic Console. If your backups are stored in Object Storage, use the Cost Analysis tools. See Monitor Your billing Data in Oracle Cloud Managing and Monitoring Oracle Cloud or Checking Your Balance and Usage in the Oracle Cloud Infrastructure documentation or .

You can also check the capacity used by your account or under a container by using cURL.

Example commands:

```
# curl -v -s -X GET
--host "X-Storage-User: service-identitydomain:userid"
```
```
-H "X-Storage-Pass: password"
https://identitydomain.storage.oraclecloud.com/auth/v1.0

Use the Auth-Token entry to get the header information:

`# curl -v -X HEAD
-H "X-Auth-Token: auth-token"
https://identitydomain.storage.oraclecloud.com/v1/service-identitydomain`

Example output (pertinent details in bold):

`< HTTP/1.1 204 No Content
< X-Account-Container-Count: 2
< X-Account-Object-Count: 567
  Server: Oracle-Storage-Cloud-Service is not blacklisted
< Server: Oracle-Storage-Cloud-Service
< X-Account-Meta-Policy-Georeplication: us2
< X-Account-Meta-Policy-Archive: arch-us2
< X-Timestamp: 1446492266.33718
< X-Account-Bytes-Used: 7884540569
< X-Account-Meta-Quota-Bytes: 536870912000
< Accept-Ranges: bytes
< X-Trans-Id: txeb61162195847a681cd6-0056a4404bga
< Date: Sun, 24 Jan 2016 03:08:59 GMT
< Connection: keep-alive
< X-Storage-Class: Standard
< X-Container-Meta-Policy-Georeplication: us2
< X-Last-Modified-Timestamp: 1446492266.33718
< Content-Type: text/plain;charset=UTF-8`

Example output for a tiering container (pertinent details in bold):

`< HTTP/1.1 204 No Content
< X-Container-Object-Count: 0
< X-Container-Write: myIdentity4.Storage.Storage_ReadWriteGroup
< Accept-Ranges: bytes
< X-Timestamp: 1531949125.70314
< X-Container-Bytes-Used: 0
< X-Trans-Id: tx0d71e235b8814b94b197b-005b4fb04ega
< Date: Wed, 18 Jul 2018 21:25:34 GMT
< Connection: keep-alive
< X-Storage-Class: Standard
< Container-Meta-Policy-Georeplication: uscom-central-1
< Container-Policies-Enabled: tiering
< Last-Modified-Timestamp: 1531949125.70314
< Content-Type: text/plain;charset=utf-8
< Server: Oracle-Storage-Cloud-Service
```
Backing Up to Oracle Database Backup Cloud Service

After you install the Oracle Database Cloud Backup Module for OCI Classic or Oracle Database Cloud Backup Module for OCI, and configure Recovery Manager (RMAN) settings, you can perform backup and restore operations using familiar RMAN commands. You’ll also use RMAN to specify retention policies, perform crosschecks, and delete backups.

Information about your cloud backups is maintained in the database control file, and in the recovery catalog if you use one.

Encryption is required to back up to Oracle Database Backup Cloud Service. You can use password encryption, Transparent Data Encryption (TDE), or dual-mode encryption, which is a combination of password and TDE.

**Note:**

Use RMAN parallelism, compression, and other best practices to speed up cloud backups and restores. For more information about optimizing performance, see the guidelines listed in Best Practices to Optimize Cloud Backup and Restore Rates.

Also note it is recommended practice to include the RMAN format string %d and %U to ensure uniqueness.

For information about performing various types of backup and restore operations, see Backing Up and Archiving Data in Oracle Database Backup and Recovery User’s Guide.

For information about RMAN commands, see About RMAN Commands in Oracle Database Backup and Recovery Reference.

**Topics**

- Backing Up to Oracle Database Backup Cloud Service
- Backing Up to Oracle Database Backup Cloud Service Using Password Encryption
- Backing Up to Oracle Database Backup Cloud Service Using Transparent Data Encryption (TDE)
- Backing Up to Oracle Database Backup Cloud Service Using Dual-Mode Encryption
- Backing Up from the Fast Recovery Area (FRA) to Oracle Database Backup Cloud Service
Backing Up to Oracle Database Backup Cloud Service

Oracle Database Backup Cloud Service can create backups to Oracle Cloud Infrastructure Classic and Oracle Cloud Infrastructure.

To create backups using Oracle Database Backup Cloud Service:

1. Install the backup module that corresponds to the destination in which backups must be stored.
   - To create backups to Oracle Cloud Infrastructure, install the Oracle Database Cloud Backup Module for OCI. Backups created using this module are stored in Oracle Cloud Infrastructure Object Storage. See Installing the Oracle Database Cloud Backup Module for OCI.
   - To create backups to Oracle Cloud Infrastructure Classic, install the Oracle Database Cloud Backup Module for OCI Classic. Backups created using this module are stored in Oracle Cloud Infrastructure Object Storage Classic. See Installing the Oracle Database Cloud Backup Module for OCI Classic.

2. Configure an RMAN channel that will be used to create the required backups.
   - To configure backups for Oracle Cloud Infrastructure or Oracle Cloud Infrastructure Classic, see Configuring Recovery Manager (RMAN) Settings.
   - To automatically move infrequently-used backups to archive storage, see Configuring Automatic Archival to Oracle Cloud Infrastructure Classic.

3. Back up the database using the **BACKUP** command.
   - Depending on the channel configured in the previous step, the backups are stored either on Oracle Cloud Infrastructure Classic or Oracle Cloud Infrastructure.

For information about the type of encryption to use when creating backups, see Backing Up to Oracle Database Backup Cloud Service Using Password Encryption, Backing Up to Oracle Database Backup Cloud Service Using Transparent Data Encryption (TDE), or Backing Up to Oracle Database Backup Cloud Service Using Dual-Mode Encryption.

**Backing Up to Oracle Database Backup Cloud Service Using Password Encryption**

You can use password encryption to back up to Oracle Database Backup Cloud Service. The password must be specified each time you back up and restore.

The following example configures password encryption for the backup and creates a backup of the entire database:

```
RMAN> SET ENCRYPTION ON IDENTIFIED BY 'my_pswd' ONLY;
RMAN> BACKUP DEVICE TYPE sbt DATABASE;
```

**Note:**

If you forget or lose the password, you won’t be able to restore the backup.
Back up using TDE you need to have a TDE wallet (TDE keystore), which is different from the OPC wallet that stores Oracle Database Backup Cloud Service credentials.

To create a TDE wallet if you don’t already have one:

1. Add the following line to the sqlnet.ora file:

```plaintext
ENCRYPTION_WALLET_LOCATION=
(SOURCE=(METHOD=FILE)
(METHOD_DATA=
(DIRECTORY=path_to_TDE_wallet)))
```

where `path_to_TDE_wallet` is the location where the TDE wallet is to be created; this must be different from the OPC wallet location.

2. Start SQL*Plus as sys:

```plaintext
sqlplus / as sysdba
```

3. Create the TDE wallet in the location specified in sqlnet.ora:

```plaintext
SQLPLUS> alter system set encryption key identified by "TDE-password";
```

where `TDE-password` is the password that must be used to open the TDE wallet.

4. Whenever the database is restarted, open the TDE wallet with the following command:

```plaintext
SQLPLUS> alter system set encryption wallet open identified by "TDE-password";
```

For complete information about TDE, see Using Transparent Data Encryption in Oracle Database Advanced Security Guide.

To back up an Oracle database that uses TDE:

1. Connect Recovery Manager (RMAN) to the target database to be backed up and configure encryption for the database:

```plaintext
RMAN> SET ENCRYPTION ON;
```

2. Back up the database:

```plaintext
RMAN> BACKUP DATABASE;
```

For information about restoring and recovering backups, see Restoring Backups from Oracle Database Backup Cloud Service.
Backing Up to Oracle Database Backup Cloud Service Using Dual-Mode Encryption

You can use dual-mode encryption to back up to Oracle Database Backup Cloud Service. Dual-mode encryption is a combination of password encryption and Transparent Data Encryption (TDE).

If TDE is configured for the Oracle database you're backing up, omit the ONLY keyword with the SET ENCRYPTION command to indicate the backup is protected with both a password and the configured transparent encryption. For example:

```
RMAN> SET ENCRYPTION ON IDENTIFIED BY 'my_pswd';
RMAN> BACKUP DEVICE TYPE sbt DATABASE;
```

**Note:**

If you forget or lose the password, you won't be able to restore the backup.

For information about restoring and recovering backups, see Restoring Backups from Oracle Database Backup Cloud Service.

Backing Up from the Fast Recovery Area (FRA) to Oracle Database Backup Cloud Service

You can back up image copies and backup sets from the fast recovery area (FRA) to Oracle Database Backup Cloud Service.

To back up image copies from FRA to Oracle Database Backup Cloud Service, use these commands:

```
RMAN> BACKUP RECOVERY AREA;
RMAN> BACKUP DEVICE TYPE sbt COPY OF DATABASE;
RMAN> BACKUP RECOVERY FILES;
RMAN> BACKUP RECOVERY FILE DESTINATION;
```

To back up backup sets from FRA to Oracle Database Backup Cloud Service, use this command:

```
RMAN> BACKUP DEVICE TYPE sbt BACKUPSET ALL;
```

For information about restoring and recovering backups, see Restoring Backups from Oracle Database Backup Cloud Service.
Restoring Backups from Oracle Database Backup Cloud Service

You can use standard Recovery Manager (RMAN) commands to perform restore and recovery operations from Oracle Database Backup Cloud Service.

A few possible scenarios are addressed here. For complete information about using RMAN to perform various types of restore and recovery operations, see Diagnosing and Responding to Failures in Oracle Database Backup and Recovery User's Guide. For information about RMAN commands, see About RMAN Commands in Oracle Database Backup and Recovery Reference. The concepts and commands in these RMAN guides are applicable to the database backed up to Oracle Database Backup Cloud Service.

Topics

- Performing General Restore and Recovery Operations
- Recovering Databases from Archive Storage
- Restoring to a New Database Host
- Creating a Data Guard Standby Database in Oracle Cloud

Performing General Restore and Recovery Operations

Oracle database backups stored in the cloud can be restored and recovered using Recovery Manager (RMAN). All RMAN restore and recovery operations are supported with cloud backups.

Before you restore backups, configure an RMAN channel that corresponds to the location where the backup that must be restored is stored. The backups can be stored in Oracle Cloud Infrastructure Object Storage or Oracle Cloud Infrastructure Object Storage Classic. For information about configuring channels, see Configuring Recovery Manager (RMAN) Settings.

For example, if password encryption was used to encrypt the backup, commands for a typical restore for the entire database would look as follows, specifying the password that was used to encrypt the backup:

```sql
RMAN> SET DECRYPTION IDENTIFIED BY 'my_pswd';
RMAN> RESTORE DATABASE;
RMAN> RECOVER DATABASE;
```

If Transparent Data Encryption (TDE) was used to encrypt the backup, you'd specify something like this:

```sql
RMAN> SET ENCRYPTION ON;
RMAN> RESTORE DATABASE;
RMAN> RECOVER DATABASE;
```
Recovering Databases from Archive Storage

Oracle database backups stored in archive storage can be restored and recovered using Recovery Manager (RMAN).

Backups can be stored in Oracle Cloud Infrastructure Archive Storage or archive storage in Oracle Cloud Infrastructure Classic. Backups stored in archive storage need to be recalled first before they can be restored. You must plan in advance for restore and recover operations using backups stored in archive storage. Use RESTORE DATABASE PREVIEW ... RECALL to initiate a recall operation for the required backups. After you begin the restore operation, if the backups are still not available to read from the archive storage, then the restore operation waits until the required backups are available. This may slow down the restore operation.

To recover a database using backups from archive storage:

1. Start RMAN and connect to the target database.
2. If the database is not mounted, then mount but do not open the database.
   For example, enter the following command:

   ```sql
   STARTUP MOUNT;
   ```

3. Depending on where the backups are stored, configure an RMAN channel that corresponds to Oracle Database Cloud Backup Module for OCI or Oracle Database Cloud Backup Module for OCI Classic. See Configuring Recovery Manager (RMAN) Settings.

4. Provide information required to decrypt the backups.
   - If password or dual-mode encryption was used to create the backups, provide the encryption password using the following syntax:

     ```sql
     RMAN> SET DECRYPTION IDENTIFIED BY encryption_password;
     ```
   - If Transparent Data Encryption (TDE) was used to create the backups, ensure that the Oracle keystore that contains the encryption key is open.

5. Preview the backups required for the restore operation using the PREVIEW option of the RESTORE command.

   The following command previews backups that will be used for the restore operation:

   ```sql
   RESTORE DATABASE PREVIEW;
   ```

   The output displays a detailed list of the backup pieces that will be used in the restore operation and the location of these backup pieces (standard Object Storage or Archive Storage). If any backup pieces are in Archive Storage, the output indicates that these are remote files.

6. Recall the required backups from archive storage using the RECALL option in the RESTORE command.
The following command recalls database backups from archive storage:

```
RESTORE DATABASE PREVIEW RECALL;
```

7. Restore and recover the database using the following commands:

```
RESTORE DATABASE;
RECOVER DATABASE;
```

Related Topics

- *Oracle Database Backup and Recovery User's Guide*

## Restoring to a New Database Host

If there’s a site failure and your database servers are down, you can use the backups in the cloud to restore to a new host. The following example shows how to restore backups from Oracle Database Backup Cloud Service to a new host.

**Note:**

If you want to restore the database to an Oracle Database Cloud Service database deployment (non-Virtual Image), see Creating a Database Deployment Using a Cloud Backup in *Using Oracle Database Cloud Service*. Otherwise, use the following steps to restore to a new host. You would also use these steps to restore to Oracle Database Cloud Service - Virtual Image database deployments.

To perform the steps in this example, the new host must have the following:

- Internet connectivity to connect to Oracle Database Backup Cloud Service
- A compatible operating system with the same endian format as the source host
- The same version of Oracle Database software as the source host

You must also know the following:

- DBID of the source database
- Password used to encrypt the backup if password-based encryption was used

To restore from a cloud backup stored using Oracle Cloud Infrastructure or Oracle Cloud Infrastructure Classic to a new host:

1. Install the Oracle Database Cloud Backup Module for OCI or Oracle Database Cloud Backup Module for OCI Classic on the new host using the same subscription credentials and custom container (if any) used for the backup. For information about installing the module, see *Downloading and Installing the Oracle Database Cloud Backup Module for OCI* or *Downloading and Installing the Oracle Database Cloud Backup Module for OCI Classic*.

   For example, with Oracle Cloud Infrastructure Classic, the service name (`serviceName`), identity domain (`-identityDomain`), user name (`-opcId`), password (`-opcPass`), and container name (`-container`), if you used a custom container,
must be the same. With Oracle Cloud Infrastructure, the tenancy OCID (-tOCID), user OCID (-uOCID), and bucket (-bucket), if you used a custom bucket, must be the same.

2. On the new host, connect to Recovery Manager (RMAN), set the decryption password, set the DBID, and restore the SPFILE.

For example:

\begin{verbatim}
rman target / 
RMAN> STARTUP NOMOUNT;
RMAN> SET DECRYPTION IDENTIFIED BY 'my_bkup_pwd';
RMAN> SET DBID=3383098001;
RMAN> RUN {
ALLOCATE CHANNEL t1 DEVICE TYPE sbt PARMS 'SBT_LIBRARY=libopc.so
ENV=(OPC_FILE=./u01/app/oracle/product/12.1.0/dbhome_1/dbs/opcDUP.ora)';
RESTORE SPFILE TO PFILE './u01/app/oracle/product/12.1.0/dbhome_1/dbs/initDUP.ora' FROM AUTOBACKUP;
}
\end{verbatim}

The same password used to encrypt the backup must be used for restore and recovery operations.

If the TDE wallet was used to encrypt the backup, the wallet must be copied to the new host and the wallet location must be set in the sqlnet.ora file before restoration is started. For details, see relevant information in My Oracle Support Doc ID 1560327.1 at http://support.oracle.com. Also, use SET ENCRYPTION ON; instead of SET DECRYPTION IDENTIFIED BY 'my_bkup_pwd'; as shown in the example above.

3. Edit the PFILE to reflect the new host, changing control file locations, create and recovery file destinations, and audit file destinations. For example, change the *_dest parameters so all destinations are correct, change the control_files parameter, and so on. If necessary, create the relevant directories on the new host.

4. Shut down the target database instance on the new host, restart the instance to the NOMOUNT state, restore the control file, and mount the database.

For example:

\begin{verbatim}
RMAN> SHUTDOWN IMMEDIATE;
RMAN> STARTUP NOMOUNT;
RMAN> RUN {
ALLOCATE CHANNEL t1 DEVICE TYPE sbt PARMS 'SBT_LIBRARY=libopc.so
ENV=(OPC_FILE=./u01/app/oracle/product/12.1.0/dbhome_1/dbs/opcDUP.ora)';
RESTORE CONTROLFILE FROM AUTOBACKUP;
}
RMAN> ALTER DATABASE MOUNT;
\end{verbatim}

5. If necessary, use the SET NEWNAMES command to define a new location for the restored data file (Oracle Database 10g and later) or database (Oracle Database 11g and later), and then start the restoration and recovery.

For example:

\begin{verbatim}
RMAN> RUN {
SET NEWNAME FOR DATABASE TO '/u02/app/oracle/oradata/DUP/%U';
ALLOCATE CHANNEL t1 DEVICE TYPE sbt PARMS 'SBT_LIBRARY=libopc.so
ENV=(OPC_FILE=./u01/app/oracle/product/12.1.0/dbhome_1/dbs/opcDUP.ora)';
ALLOCATE CHANNEL t2 DEVICE TYPE sbt PARMS 'SBT_LIBRARY=libopc.so
ENV=(OPC_FILE=./u01/app/oracle/product/12.1.0/dbhome_1/dbs/opcDUP.ora)';
ALLOCATE CHANNEL t3 DEVICE TYPE sbt PARMS 'SBT_LIBRARY=libopc.so
\end{verbatim}
ENV=(OPC_FILE=/u01/app/oracle/product/12.1.0/dbhome_1/dbs/opcDUP.ora);

RESTORE DATABASE;
SWITCH DATAFILE ALL;
SQL "ALTER DATABASE RENAME FILE '+DATA/ASMDEMO1/ONLINELOG/
group_3.263.873380343' TO '/u04/app/oracle/redo/redo03.log'';"
SQL "ALTER DATABASE RENAME FILE '+FRA/ASMDEMO1/ONLINELOG/
group_3.260.873380343' TO '/u04/app/oracle/redo/redo01.log'';"
SQL "ALTER DATABASE RENAME FILE '+DATA/ASMDEMO1/ONLINELOG/
group_2.262.873380341' TO '/u04/app/oracle/redo/redo02.log'';"
SQL "ALTER DATABASE RENAME FILE '+FRA/ASMDEMO1/ONLINELOG/
group_2.259.873380341' TO '/u04/app/oracle/redo/redo04.log'';"
SQL "ALTER DATABASE RENAME FILE '+DATA/ASMDEMO1/ONLINELOG/
group_1.261.873380341' TO '/u04/app/oracle/redo/redo05.log'';"
SQL "ALTER DATABASE RENAME FILE '+FRA/ASMDEMO1/ONLINELOG/
group_1.258.873380341' TO '/u04/app/oracle/redo/redo06.log'';"

6. Find the system change number (SCN) to make the database consistent:
   RMAN> RESTORE DATABASE PREVIEW DEVICE TYPE SBT;

   The output includes the name and location of backup pieces that will be used when restoring the database.

7. Recall any required backup pieces that were archived.
   If the RESTORE...PREVIEW command output contains a section named List of remote backup files, it means that some required backup pieces were archived. Recall these backup pieces using the following command:

   RMAN> RESTORE DATABASE PREVIEW RECALL DEVICE TYPE SBT;

8. Restore the database using the following command:

   RESTORE DATABASE DEVICE TYPE SBT;

9. Recover the database to that point:
   RMAN> RECOVER DATABASE DEVICE TYPE SBT UNTIL SCN scn;

   where scn is the SCN identified in the previous step.

   For Oracle Database 12c Release 2 (12.2) and higher, you can use the RECOVER DATABASE UNTIL AVAILABLE REDO command.

10. Open the database with the RESETLOGS option after restore and recovery is complete:
    RMAN> ALTER DATABASE OPEN RESETLOGS;

---

Creating a Data Guard Standby Database in Oracle Cloud

To deploy a disaster recovery site for an on-premises production database using Oracle Database Cloud Service or Oracle Database Exadata Cloud Service, you need to create a standby database in the cloud to be used with Oracle Data Guard or Oracle Active Data Guard.

One way to create a standby database is to restore the backup performed from the on-premises production database. For detailed information, see Appendix I in the Disaster
Recovery to the Oracle Cloud white paper. The appendix describes how to create a database from Oracle Database Backup Cloud Service.
Troubleshooting Oracle Database Backup Cloud Service

You might encounter some problems when you use Oracle Database Backup Cloud Service. This section lists common problems and their possible solutions. Also see the Oracle Database Backup Cloud Service FAQ (My Oracle Support Doc ID 1640149.1) and Cloud Backup Performance Analysis (My Oracle Support Doc ID 2078576.1) at http://support.oracle.com.

Topics

• Best Practices to Optimize Cloud Backup and Restore Rates
• Problems with Installing the Backup Module
• Problems with Backing Up and Restoring
• Problems with Connectivity

Best Practices to Optimize Cloud Backup and Restore Rates

Because cloud backups are sent over the public Internet, backup performance is affected by network bandwidth limitations. Use RMAN parallelism and compression to speed up cloud backups and restores.

To optimize performance:

• Use multiple RMAN channels for higher parallelism, which results in full utilization of the network. You can configure as many RMAN channels as you want. For example, the following configuration uses eight channels in parallel to back up to the cloud:

RMAN> CONFIGURE DEVICE TYPE sbt PARALLELISM 8;

Try increasing the parallelism until you find the optimal transfer rate.

• Use an RMAN compression level of MEDIUM.
• Use multisection backups. With these, multiple RMAN channels are used in parallel to back up large data files in separate sections.

You create multisection backups by specifying the SECTION SIZE parameter with the BACKUP command. For example, the following command specifies a backup section size of 1 GB:

RMAN> BACKUP DEVICE TYPE sbt DATABASE SECTION SIZE 1g;

• Use a backup strategy of weekly full and daily incremental backups. This results in faster backups and could save a significant amount of network bandwidth. Use the
RMAN fast incremental backup feature (based on block change tracking) to optimize the performance of your daily incremental backups.

- Use a recovery catalog to store long-term backups. For information about recovery catalogs, see Managing a Recovery Catalog in Oracle Database Backup and Recovery User’s Guide.

Note:
You can test network throughput by using the throughput measurement tool. See Testing Network Throughput in Managing and Monitoring Oracle Cloud.

Problems with Installing the Backup Module

The following solutions apply if you run into issues when you install the Oracle Database Cloud Backup Module.

For general information about installation, see Installing the Oracle Database Cloud Backup Module for OCI or Installing the Oracle Database Cloud Backup Module for OCI Classic.

Note:
In addition to what’s listed in this section, also check the following:
- **Java version:** JDK 1.7 or later is required
- **Identity domain name or service name:** Make sure they’re spelled correctly
- **Backup module:** Make sure you’ve downloaded the latest backup module from Oracle Technology Network (OTN)
- **Proxy or firewall issues:** Make sure your proxy is set up correctly, and you can reach general URLs from your system

I get an HTTP response code error when I run the installer for Oracle Cloud Infrastructure Classic

Specific error:

Server returned HTTP response code: 504 for URL:
https://identityDomain.storage.oraclecloud.com/v1/storage-identityDomain/?format=xml

Use the `-host` parameter when you run the installer, instead of the `-serviceName` and `-identityDomain` parameters. For example:

-host https://abc.storage.oraclecloud.com/v1/hr-abc

Exclude `/?format=xml` at the end of the URL. For information about these parameters, see Parameters Used to Run the Oracle Database Cloud Backup Module for OCI Classic Installer.
I get a **ConfigFile was not specified** error when I run the installer

Specific error:

ConfigFile was not specified, and a default location could not be determined because ORACLE_HOME and ORACLE_SID are not both set.

Set **ORACLE_HOME** and **ORACLE_SID** and rerun the installer.

I get a **Specified directory does not exist** error when I run the installer

Specific error:

Specified directory /home/oracle/OPC/lib does not exist.

The directory specified for the `-libDir` parameter does not exist. Create the directory and rerun the installer.

I get a **java.io.IOException** or **java.io.FileNotFound** error when I run the installer

For example:

```java
java.io.IOException: Server returned HTTP response code: 401 for the URL URL-name
```

The installer can't connect to Oracle Cloud with the information you provided. Try the following:

- Make sure the user name, password, service name, and identity domain used to run the installer are correct. With Oracle Cloud Infrastructure, make sure that the user OCID, tenancy OCID, fingerprint, and keys are correct.

  Enclose the user name and password in single quotes, for example 'myAccount@myCompany.com' and 'opc_pswd'. On Windows systems, use double quotes if the user name or password contains special characters.

  Fix any errors and rerun the installer. If the information you provided is correct, contact Oracle Support to verify your account information.

**Note:**

If you have a pre-paid metered subscription for Oracle Cloud Infrastructure Classic, the default service name is **Storage** (case sensitive). This is the name you'll use for the `-serviceName` parameter when you install the backup module.

- Check connectivity and see if you can reach the cloud storage endpoint URL from your database server. For example:

  ```bash
  $ ping storage.us2.oraclecloud.com
  PING storage.us2.oraclecloud.com (160.34.0.51): 56 data bytes
  64 bytes from 160.34.0.51: icmp_seq=0 ttl=239 time=63.738 ms
  64 bytes from 160.34.0.51: icmp_seq=1 ttl=239 time=67.288 ms
  ```
I get a **Could not authenticate or 403 Forbidden** error when I run the installer for **Oracle Cloud Infrastructure Classic**

This could be because you need to select a data center. See [How to Begin with Oracle Database Backup Cloud Service Subscriptions](#).

The replication policy must be set before you run the backup module installer. Otherwise you'll get errors such as **Could not authenticate to Oracle Database Cloud Backup Module** or **403 Forbidden**. Set the replication policy and wait at least 10 minutes for synchronization to complete before you retry the installation.

I get a **Failed to load Media Management Library** error


If the problem persists, run the following operating system command (all platforms):

```
sbttest -f foo.txt -libname full-path-to-libopc|oraopc-library
```

The output shows why the module is not being loaded.

I'm using a Solaris 64-bit operating system and keep getting **ORA-27211 - Failed to load Media Management Library**

Installation is most likely failing because the **libc.so.1** file does not exist in your environment. Confirm this by running the following operating system command:

```
sbttool -f foo.txt -libname full-path-to-libopc.so
```

To resolve the issue, set the operating system variable **LD_LIBRARY_PATH_64** to the 64-bit library path that has the **libc.so.1** file. If that doesn't resolve the issue and you're using an Oracle Solaris release earlier than Solaris 10 Update 10 (s10u10), upgrade your system to at least s10u10.

I get an **Exception in thread** error when I run the installer

Specific error:

```
Exception in thread "main" java.io.FileNotFoundException: orclhome/dbs/opcdb1210.ora (No such file or directory)
```

The installer can't create the configuration file under the **ORACLE_HOME/dbs** directory. Make sure the directory is accessible. Also make sure the path for **ORACLE_HOME** is set correctly.

I get a **PKIX path building failed: unable to find valid certification path to requested target** error when I run the installer

Your database server's Java keystore does not have the SSL certificate of Oracle Cloud. You can work around this problem by using the **-no-check-certificate** option from the command line.
The wallet directory can't be created by the installer

Make sure the path you specified is correct, and the user account (oracle, for instance) has read/write/execute (rwx) access to that path. Alternatively, create a wallet directory and use that as the location for the \(-walletDir\) parameter.

I have a pre-paid metered subscription and don't know what service name to use to install the Oracle Database Cloud Backup Module for OCI Classic

If you have a pre-paid metered subscription, the service name is Storage (case sensitive). This is the name you'll use for the \(-serviceName\) parameter when you install the backup module.

Problems with Backing Up and Restoring

The following solutions apply if you run into issues when you perform cloud backup and restore operations.

For general information about cloud backups and restores, see Backing Up to Oracle Database Backup Cloud Service and Restoring Backups from Oracle Database Backup Cloud Service.

I get an RMAN encryption error when I try to back up

Specific error:

RMAN-03009: failure of backup command on ORA_SBT_TAPE_1 channel at 08/15/2014 14:00:43
ORA-27030: skgfwrt: sbtwrite2 returned error
ORA-19511: non RMAN, but media manager or vendor specific failure, error text:

KBHS-01602: backup piece 14p0jso8_1_1 is not encrypted

Backups must be encrypted before they can be sent to the cloud. Specify encryption and try backing up again.

I changed my password for Oracle Cloud and now my backups to Oracle Cloud Infrastructure Classic are failing

When you change your password for Oracle Cloud, you also need to update your password in the wallet used for backing up to Oracle Cloud Infrastructure Classic. Credentials in the wallet are used to authenticate to the cloud before backup data is sent. If the password isn't updated in the wallet, the backup fails because of the incorrect password.

To update the password in the wallet, rerun the Oracle Database Cloud Backup Module for OCI Classic installer with the new credentials. You can omit the \(-libdir\) parameter if you don't want to download the library. For more information about running the installer, see Downloading and Installing the Oracle Database Cloud Backup Module for OCI Classic.

If you're using Oracle Database Cloud Service or Oracle Database Exadata Cloud Service and use object storage for backups, you need to update the password used for backing up after you change your password for Oracle Cloud. For Database Cloud Service, see Updating the Password for Backing Up to the Storage Cloud in Using Oracle Database Cloud Service. For Exadata Cloud Service, see Updating the
Password for Backing Up to the Storage Cloud in *Using Oracle Database Exadata Cloud Service*.

**I get a Request Entity Too Large error when I try to back up**

When you subscribe to Oracle Database Backup Cloud Service, you purchase the amount of storage capacity you want. If you reach your storage capacity limit and try to back up your database, your backup will fail. An error related to this might look as follows:

```
RMAN-00571: ==============================================================
RMAN-00569: =============== ERROR MESSAGE STACK FOLLOWS ===============
RMAN-00571: ==============================================================
RMAN-03009: failure of backup command on cl channel at 12/02/2014 16:35:58
ORA-27030: skgfwrt: sbtwrite2 returned error
ORA-19511: Error received from media manager layer, error text:
KBHS-01404: See trace file /u01/app/oracle/admin/proddb/diag/rdbms/proddb/trace/sbtio_5884_123456.log for details
KBHS-00700: HTTP response error 'Request Entity Too Large'
```

You can quickly increase the limit by purchasing more storage capacity on demand. Once you buy more capacity, you can continue doing backups. You can also use the RMAN **DELETE** operation to free up space. As a best practice you should set up a proper retention period and periodically run RMAN backup management operations such as **CROSSCHECK**, **OBsolete**, and **DELETE**.

You can monitor how much storage capacity you've used by viewing detailed metrics. You can also check the capacity used by your account or under a container by using cURL. See [Monitoring Your Storage Capacity](#).

**I'm on a Windows system and keep getting System or Media Management Loading errors when I try to back up. How do I resolve this?**


**How do I get more information when a backup fails?**

Add the following parameter to the **opcSID.ora** configuration file to enable tracing, and then rerun the RMAN command:

```
_OPC_TRACE_LEVEL=100
```

This adds trace data to the **sbtio.log** file. To disable tracing, remove the **_OPC_TRACE_LEVEL** parameter or set the value to 0.

For information about the **opcSID.ora** configuration file, see [Files Created When the Oracle Database Cloud Backup Module for OCI Classic is Installed](#).

**I get an error when I use password-based encryption for my backup**

Specific error:

```
RMAN-03009: failure of backup command on ORA_SBT_TAPE_1 channel at 08/15/2014 11:10:57
ORA-19914: unable to encrypt backup
ORA-28361: master key not yet set
```
You probably didn’t add the **ONLY** parameter when you specified password encryption. It should be something like this:

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

I used password-based encryption for my backup and don’t remember the password — how do I restore the backup?

Unfortunately, you can’t. The password used to encrypt a backup must also be used to decrypt it for restore and recovery operations. If you forget or lose the password, you cannot restore the backup.

**RMAN restores from another location, not the cloud**

Use `SHOW ALL` to confirm that RMAN is configured to use Oracle Database Backup Cloud Service as the backup destination. See [Configuring Recovery Manager (RMAN) Settings](#). Also check for proper syntax.

---

**Problems with Connectivity**

The following solution applies if you run into issues when you try to connect to Oracle Database Backup Cloud Service.

**I get connectivity errors from my database server**

This could be caused by any number of things, including network bandwidth issues and incorrect proxy settings. Test to see if you can reach general URLs from your system.