

Oracle Secure Backup

Getting Started

with Cloud Storage Devices


ORACLE WHITE PAPER | FEBRUARY 2018





Disclaimer

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle.



Disclaimer	0
Introduction	1
Before you begin	2
Subscribe Oracle Object Storage cloud service	2
Get your Identity Domain and login credentials	2
Download cloud server CA certificate chain	3
Install OSB software version 12.2 on Admin, media and client	4
Create Wallet and Import certificates	4
Create Cloud storage device	5
Test your backup	7



Introduction

Oracle Secure Backup 12.2 is Oracle's media management solution, it provides centralized backup management for heterogeneous file systems and the Oracle database to disk, tape and cloud. Cloud Storage can be used to backup data from cloud compute instances or for offsite storage of on-premises data, providing a valid alternative to vaulting services. Backup images are stored, in encrypted form, in Oracle Cloud Infrastructure Storage Classic containers, the encryption keys are stored in the Oracle Secure Backup administrative server. Containers come in two types, Standard Object Storage and Archive Storage. Standard containers provide the faster access to data in case of restore, Archive containers are for longer term retention, infrequently accessed data; the cost for storing data in Archive containers is cheaper compared to Standard containers, but there is a delay of up to 4 hours to retrieve the data in case of restore. This paper is for users already familiar with Oracle Secure Backup currently using tape or disk devices that want to get started with the new Cloud Storage devices quickly.

Before you begin

- To setup OSB to use Oracle Cloud Storage Classic containers as target, perform the following steps.
- Subscribe to Oracle Object Storage cloud service.
- Get your login credentials and identity domain
- Download cloud server CA certificate chain trust points
- Install OSB software version 12.2 on Admin, Media Server and Client
- Create the wallet and import the certificates
- Create the Cloud Storage Device
- Test your backup

Subscribe Oracle Object Storage cloud service

This is the basic requirement to access Oracle object storage services. You can subscribe for a paid or trial service from following link.

https://cloud.oracle.com/en_US/storage-classic

The service offers different options with and without replication. You can also subscribe for Archive storage service that provides a cheaper storage for long term retention. The details of each services and associated cost are available at above mentioned link.

Get your Identity Domain and login credentials

Once you subscribe to cloud services, Oracle creates a unique identifier for all of your services. This is referred as an Identity Domain. Oracle also asks you to create an identity domain administrator user for managing your cloud services and authorized users.

After you receive your Identity Domain and user credentials, you can use it to create login account for other users that would need to access the services. For accessing Storage services from OSB, it is recommended that you create another user with storage administrator role. This user should also have Storage Read Write role.

The details of adding new user and roles are available at below link

<https://docs.oracle.com/en/cloud/get-started/subscriptions-cloud/csgsg/adding-users-and-assigning-roles.html>

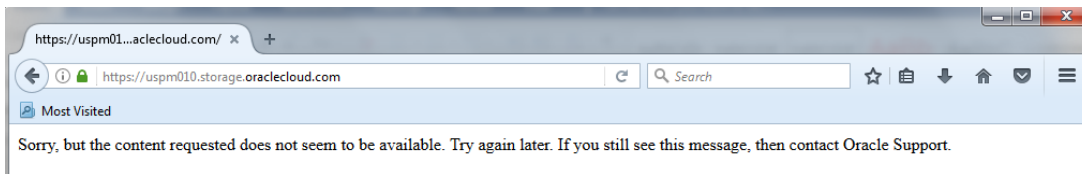
Download cloud server CA certificate chain trust points

OSB uses the cloud server CA certificate to make SSL connections to the cloud storage services. You are required to download the CA certificate chain and save it on the OSB admin and media servers. To download the certificates follow following steps

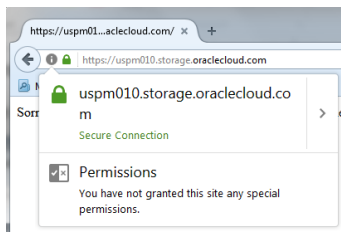
1. Open your web browser and visit following link (we used Firefox in the examples below)

`https://<identity domain>.storage.oraclecloud.com`

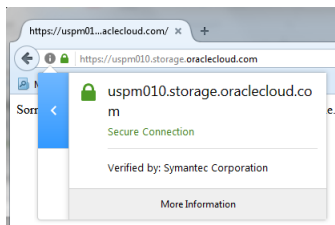
The browsers shows a message as below



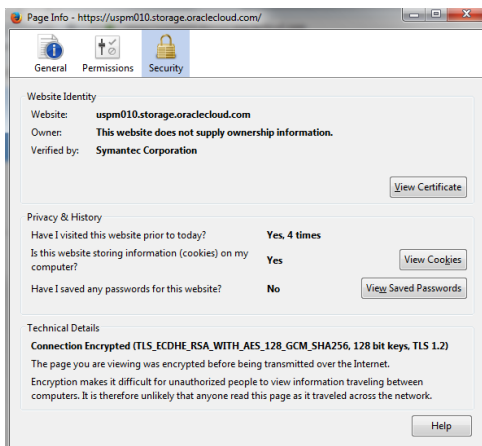
2. Click on green security lock sign and proceed to view more information and certificate



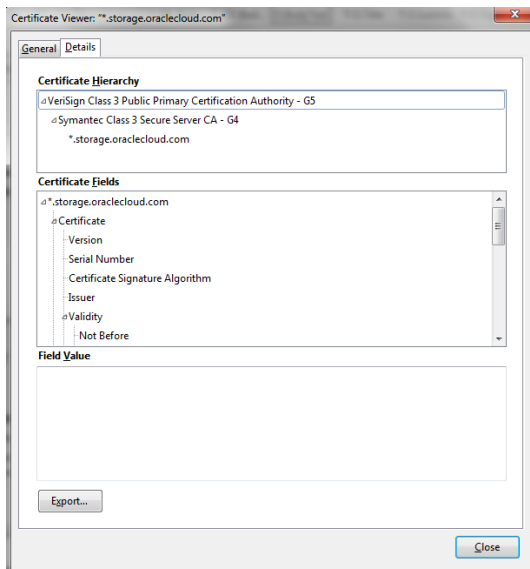
4. Click on arrow to proceed to see more information as below



5. Click on more Information to view dialog box as below



6. Click on view certificate and select the Details tab to see certificate details.



7. Select the first two certificates on the chain one at a time and click export.
8. Save the exported certificate file to local media.

Install OSB software version 12.2 on Admin, media and client

Download OSB 12.2 from [OTN](#)

You can now install OSB software version 12.2 on your admin server, media server and client. Refer to Oracle Secure backup Installation document for details on installation or upgrade.

Create Wallet and Import Certificate Trust Points

Once OSB installation is complete, copy the downloaded certificate trust points to your admin and media servers and then create a wallet and import the certificates into it using the OSB certificate manager command "obcm". You must specify a password when creating the wallet, remember the password you entered as you will need at a later time for importing the certificates.

Usage: **obcm wallet [--create/-c] [--add/-a <trust point path>]**

[--cloudwallet/-L | --wpath/-w <wallet path>]

- c: Create wallet
- a: Add trust point to wallet
- L: Create/Add to Cloud wallet
- w: Create/Add to <wallet path>

Create a wallet using following command. You are prompted for a new password.

```
# obcm wallet --create --cloudwallet
```

Wallet Password: xxxx

Wallet password (again): xxxx

Wallet has been created.

Add the certificates to the wallet as below specifying the certificate files you downloaded and copied to the admin and media servers.

```
# obcm wallet --cloudwallet --add /home/opc/SymantecClass3SecureServerCA-G4.crt
```

Wallet password:

Trust point has been imported into wallet.

```
# obcm wallet --cloudwallet --add /home/opc/VeriSignClass3PublicPrimaryCertificationAuthority-G5.crt
```

Wallet password:

Trust point has been imported into wallet.

Create Cloud storage device

Use the familiar mkdev command to create a new cloud storage device as below. You will be prompted to provide your cloud account password. The container must not exist as OSB will create it for you and you have to specify the object (for fast restore access) or archive (for long term retention, infrequently accessed data) class. There is a 4 hour delay to get data back from an archive container in case of restore.

```
# obtool mkdev --type cloudstorage --identitydomain <your identity domain> \  
  --url <identity domain>.storage.oraclecloud.com --mediaserver <name of media server>  
  --user <user name> --querypassphrase\  
  --container <container name> <device name>  
  --storageclass <object | archive>
```

Password: xxxx

It is also recommended to adjust the cloud transfer timeout to 10 seconds using the following command

```
# obtool setp cloud/transfertimeout 10sec
```


Alternatively you can use the OSB webtool, select Configure → Basic → Devices

The screenshot shows the Oracle Secure Backup web interface. The navigation path is: Home > Configure > Manage > Backup > Restore > Basic > Users > Hosts > Devices. The 'Devices' page is displayed, showing a table of existing devices and sections for Active, Pending, and Completed jobs. The table has columns for ID, Type, Level, Scheduled time, and Status. The 'Active Jobs' section shows 0 jobs in the last 24 hours. The 'Pending Jobs' section shows 0 jobs in the last 24 hours. The 'Completed Jobs' section shows 0 jobs in the last 24 hours. The 'Devices' section shows a table with columns for Type (DTE), Name, and State. The table contains two rows: cloud storage (cloudstor1) in service and cloud storage (cloudstor2) in service. There is a 'Refresh' button at the bottom right of the page.


The device page is displayed, click **Add** to create a new device

The screenshot shows the Oracle Secure Backup web interface. The navigation path is: Home > Configure > Manage > Backup > Restore > Configure > Devices. The 'Configure > Devices' page is displayed, showing a table of existing devices and buttons for Add, Edit, Remove, Rename, Verify, Show Properties, Ping, and Discover Devices. The table has columns for Type (DTE), Status, and Device Name. The table contains two rows: cloud (storage) in service (cloudstor1) and cloud (storage) in service (cloudstor2). There is an 'Add' button at the bottom left of the page.

Select the Type: cloudstorage, enter the Device name, select Mediaserver and Storage class (Object or Archive).

The screenshot shows the Oracle Secure Backup web interface. The navigation path is: Configure > Device > cloudstore3. The 'Configure > Device > cloudstore3' page is displayed, showing a form for configuring a new device. The 'Device' field is set to 'cloudstore3'. The 'Type' is 'cloudstorage'. The 'Status' is 'in service'. The 'Debug mode' is 'no'. The 'Mediaserver' is 'oow2017ra osb'. The 'Storage class' is 'object'. The 'Capacity' is '(not set)'. The 'User name' is 'mycloudaccount'. The 'Password' is masked with '*****'. The 'Container' is 'Container3'. The 'Segment size' is '(system default) MB'. The 'Streams per job' is '(system default)'. The 'Concurrent jobs' is '4'. The 'Blocking factor' is '(system default)'. The 'Free space goal percentage' is '(system default)'. The 'Proxy URL' is 'mydomain.storage.oraclecloud.com'. The 'Identity domain' is 'mydomain'. There are 'Apply', 'OK', and 'Cancel' buttons at the bottom of the form.

Enter the cloud account name and password, the URL can be obtained clicking on the Storage Classic service type link in the Oracle Cloud Dashboard and looking for the REST Endpoint, use only the hostname component that usually has the form **domain-id.storage.oraclecloud.com**



You can verify your cloud device has been set up properly and is accessible using the pingdev obtool command:

obtool pingdev <clouddevice>

For additional options refer to the [Configuring Cloud Storage Devices](#) chapter in the Oracle Secure Backup 12.2 Installation and Configuration Guide.

Test your backup

Now you can create a dataset and submit backup to new configured cloud storage device. For added functionality like manual and automate copy (staging) of backup images refer to Oracle Secure backup administrator guide.







Oracle Corporation, World Headquarters

500 Oracle Parkway
Redwood Shores, CA 94065, USA

Worldwide Inquiries

Phone: +1.650.506.7000
Fax: +1.650.506.7200

CONNECT WITH US

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

Hardware and Software, Engineered to Work Together

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

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

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group. 0218

 | Oracle is committed to developing practices and products that help protect the environment