Observability and Management: Configure Service Connectors

Lab 21-1 Practices

Get Started

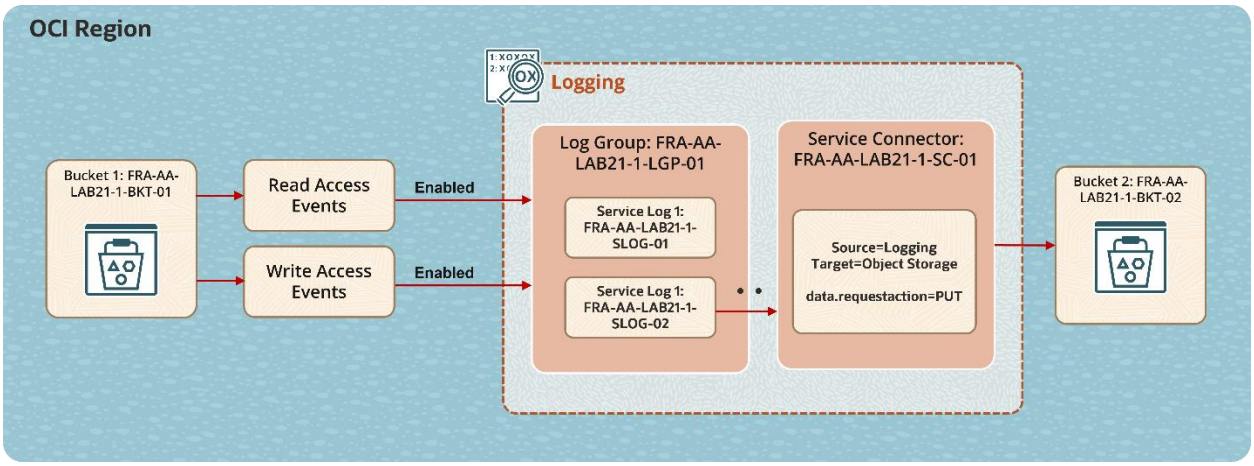
Overview

A service connector specifies the source logs, optional filtering/processing, execution frequency, and the destination Object Storage bucket. In this lab, we will enable service logs for Object Storage events and export them into another Object Storage bucket.

In this lab, you will:

a. Enable service logs

b. Export logs using service connectors



Assumptions

- You must be familiar with navigating the OCI Console.
- In this lab, Germany Central (Frankfurt) is considered as your region.

Set Up the Environment

In this practice, you will create an automated job to export your log data into the Object Storage bucket for long-term storage and archive. The Oracle Cloud Infrastructure (OCI) makes this easy via service connectors, which provide a framework for creating jobs to filter, process, and move log data from Logging to Object Storage.

Task 1: Create Object Storage Buckets

An Object Storage bucket is a logical container for storing objects. A bucket is associated with a single compartment that has policies to determine what actions a user can perform on a bucket and on all the objects in the bucket. The objects can store any type of data regardless of the content type. In this task, you will create two buckets: one for enabling logging and another for archiving logs.

1. Sign in to your Oracle Cloud Infrastructure (OCI) account.
2. In the console ribbon at the top of the screen, click the Region icon to expand the menu and select **Germany Central (Frankfurt)**.
3. From the navigation menu, select **Storage**. Under **Object Storage & Archive Storage**, click **Buckets**.
4. Click **Create Bucket**.
5. In the **Create Bucket** dialog box, enter `FRA-AA-LAB21-1-BKT-01-xxx` in the **Name** field.

   Please specify a random number in place of xxx to make it unique.
6. In the **Default Storage Tier** field, select **Standard**.
7. In the **Encryption** field, select **Encrypt using Oracle managed keys**.
8. Keep the rest of the options as default and click **Create**.

   You will now create a second bucket, which will be used as the archive bucket to move logs generated for read events occurred for the first bucket.
9. Navigate back to the **Buckets** page from the navigation menu.
10. Click **Create Bucket**.

11. In the **Create Bucket** dialog box, enter `FRA-AA-LAB21-1-BKT-02-xxx` in the **Name** field.

    Please specify a random number in place of xxx to make it unique.

12. In the **Default Storage Tier** field, select **Standard.**

    Note: The Default Storage Tier can also be selected as Archive; however, in this lab, you will select Standard to immediately download the transitioned log. An object in Archive Storage Tier needs to be restored first before it can be downloaded.

13. Keep the rest of the options as default and click **Create**.

Enable Service Logs

In this practice, you will enable automatic log collection for Object Storage activity (read, write) for the bucket created earlier.

Task 1: Create a Log Group

1. From the navigation menu, select **Observability & Management**. Under **Logging**, click **Log Groups**.
2. From the left navigation panel, ensure that you are in the compartment assigned to you.
3. Click **Create Log Group**.
4. In the **Create Log Group** dialog box, ensure that the **Compartment** field is populated with <*your compartment*>.
5. In the **Name** field, enter `FRA-AA-LAB21-1-LGP-01`.
6. In the **Description** field, enter a brief description.
7. Click **Create**.

Task 2: Enable Object Storage Log

In this task, you will enable logging on the Object Storage bucket created earlier.

1. From the navigation menu, select **Observability & Management**. Under **Logging**, click **Log Groups**.
2. From the left navigation panel, ensure that you are in the compartment assigned to you.
3. Click the **FRA-AA-LAB21-1-LGP-01** log group.
4. From the left navigation panel, select **Logs**.
5. Click **Enable service log**.

6. In the **Enable Resource Log** dialog box, populate the following information:
    - **Resource Compartment**: <*your compartment*>
    - **Service**: Object Storage
    - **Resource**: `FRA-AA-LAB21-1-BKT-01-xxx`
    - **Log Category**: Read Access Events
    - **Log Name**: `FRA-AA-LAB21-1-SLOG-01`
7. Click **Enable Log**.
8. Review the log details page. It may take a couple minutes for the service to complete configurations. The Status under Log Information should be Active.
9. Navigate back to the **Logs** page and click **Enable service log**.
10. In the **Enable Resource Log** dialog box, populate the following information:
    - **Resource Compartment**: <*your compartment*>
    - **Service**: Object Storage
    - **Resource**: `FRA-AA-LAB21-1-BKT-01-xxx`
    - **Log Category**: Write Access Events
    - **Log Name**: `FRA-AA-LAB21-1-SLOG-02`
11. Click **Enable Log**.
12. Review the log details page. It may take a couple minutes for the service to complete configurations. The Status under Log Information should be **Active**.
13. From the navigation menu, select **Storage**. Under **Object Storage & Archive Storage**, click **Buckets**.
14. Click the **FRA-AA-LAB21-1-BKT-01-xxx bucket**.
15. Under **Resources** in the left navigation panel, click **Logs**.
16. Verify that the status of Read Access Events is Active and Enabled with Log Group FRA-AA-LAB21-1-LGP-01 and Log Name FRA-AA-LAB21-1-SLOG-01.

17. Verify that the status of Write Access Events is Active and Enabled with Log Group FRA-AA-LAB21-1-LGP-01 and Log Name FRA-AA-LAB21-1-SLOG-02.

18. Under **Resources** in the left navigation panel, click **Objects**.

19. Verify that the bucket is empty.

    Note: Leave the bucket empty for now. In a later task, you will upload a few objects into the bucket that generates write events and those logs (applied with a filter) will be transitioned into the second Object Storage bucket.

Export Logs Using Service Connectors

In this practice, you will explore the contents of your logs using the built-in search capabilities provided by the Logging service. This will validate that the logging is working for FRA-AA-LAB21-1-BKT-01.

In a later task, you will configure a service connector to export logs into second Bucket FRA-AA-LAB21-1-BKT-02.

Task 1: Validate Logs with Log Search

1. From the navigation menu, select **Observability & Management**. Under **Logging**, click **Search**. You will now create search criteria and look for logs pertaining to your bucket, FRA-AA-LAB21-1-BKT-01-xxx.

2. Click **Select logs to search** text field.

3. In the **Select logs to search** field, click **x** to remove <*your compartment*> if selected by default.

4. Expand the **(root)** compartment under the **Compartment** column and select <*your compartment*> from the Compartment list.

   Note: Do not click the plus (+) sign. Click the compartment name only.

   This step will bring up the log groups in that compartment without including the compartment itself as part of the search criteria. You don't want the compartment itself included, because you don't want all the logs for that compartment in the search results.

5. In the **Log Groups** column, select the **FRA-AA-LAB21-1-LGP-01** log group, but again, click the name only without clicking the plus sign. This will bring up the logs for that log group.

6. In the **Logs** column, select **FRA-AA-LAB21-1-SLOG-01**.

7. This time, click the plus (+) sign to add it as the only search criteria. The **Select logs to search** field at the top of the dialog box will be updated.

8. Click **Continue** to execute the search.

9. Verify that the graph shows the corresponding log records. If the graph is not displayed, change the **Filter by time** field to **Past hour**.

10. In the **Custom filters** field at the top of the Search area, enter **`data.message =`**. You can then select from the list to further refine your search. Select one of the log records listed that contains the specific message.

    The graph and log section will be updated based on the selected `data.message`.

Task 2: Create a Service Connector

1. From the navigation menu, select **Observability & Management**. Under **Logging**, click **Service Connectors**.
2. Click **Create Service Connectors**.
3. In the **Create service connectors** dialog box, populate the following information:
    - **Connector name**: `FRA-AA-LAB21-1-SC-01`
    - **Description**: <*description*>
    - **Resource compartment**: <*your compartment*>
    - **Source**: Logging
    - **Target**: Object Storage
4. In the **Configure source** section, ensure that the following information is populated:
    - **Compartment**: <*your compartment*>
    - **Log Group**: FRA-AA-LAB21-1-LGP-01
    - **Logs**: FRA-AA-LAB21-1-SLOG-02
5. Wait a few seconds for **Log filter task** section to load. Then in the **Property** field, enter **`data.requestAction`**.
6. In the **Operator** field, select **=**.
7. In the **Value** field, enter **`PUT`** and press the **Enter** key.

8. Keep the **Configure task** section as default. In the **Configure target** section, populate the following information:

   - **Compartment**: <*your compartment*>
   - **Bucket**: `FRA-AA-LAB21-1-BKT-02-xxx`

   Note: Do not click **Create** in the "Create default policy allowing this service connector to write to Object Storage in compartment <*your compartment*>" message box. The policies are already added to your compartment.

9. Click **Create**.

10. Navigate to the **Service Connectors** page using the breadcrumb list.

11. Verify that the Status column shows **Active** for FRA-AA-LAB21-1-SC-01, the Source column shows as **Logging**, and the Target column as **Object Storage**.

    Note: The service connector is created to move log data that contains the data.requestAction=PUT into the Object Storage bucket- **FRA-AA-LAB21-1-BKT-02-xxx**. The log message is generated when an object is uploaded in the bucket. To generate a specific log with PUT action, you will upload objects into the bucket using OCI CLI.

Task 3: Upload Objects into Object Storage Bucket

1. In the OCI Console header, click the **Cloud Shell** icon next to the Region icon.

2. Once the Cloud Shell launches, run the following commands:

```
$ echo "Object Storage Bucket Write Event 1" >> labobject1.txt
$ echo "Object Storage Bucket Write Event 2" >> labobject2.txt
$ echo "Object Storage Bucket Write Event 3" >> labobject3.txt
```

   Reminder: Do not include the $ symbol when pasting code into Cloud Shell.

3. Run the following command to verify if the files are created successfully:

```
$ ls
```

   The three files, `labobject1.txt`, `labobject2.txt`, and `labobject3.txt`, should be listed.

4. Run the following command to upload the **`labobject1.txt`** file into the bucket:

```
$ oci os object put --bucket-name="FRA-AA-LAB21-1-BKT-01-xxx" --
name labobject1.txt --file ./labobject1.txt
```

An output in JSON format should be returned with etag, last-modified, opc-content-md5 along with each of their values.

5. Run the following command to upload the `labobject2.txt` file:

```
$ oci os object put --bucket-name="FRA-AA-LAB21-1-BKT-01-
<User_Id>" --name labobject2.txt --file ./labobject2.txt
```

6. Run the following command to upload the `labobject3.txt` file:

```
$ oci os object put --bucket-name="FRA-AA-LAB21-1-BKT-01-xxx" --
name labobject3.txt --file ./labobject3.txt
```

7. Once done, close the Cloud Shell window.

Task 4: Verify the Logs Archived by Using Service Connector

The log content archived to Object Storage is aggregated via batches (default every seven minutes) and stored in `.gz` format. The timestamps allows easy retrieval by time ranges. In this task, you will locate the archived content and optionally download/extract/view to validate the storage integrity.

Note: This task needs to be run after 7 minutes, which is the rollover time for uploading files into the Object Storage bucket.

1. From the navigation menu, select **Storage**. Under **Object Storage & Archive Storage**, click **Buckets**.

2. Click the **FRA-AA-LAB21-1-BKT-01-xxx** bucket.

3. Verify that the new objects, `labobject1.txt`, `labobject2.txt`, and `labobject3.txt`, are uploaded and displayed.

4. Navigate back to the **Object Storage** page by using the breadcrumb list and click the **FRA-AA-LAB21-1-BKT-02-xxx** bucket.

5. Verify that there is a folder created for the service connector, and expand the bucket contents to view archive content in timestamped `log.gz` format.

   Note: It may take a few minutes after creating the connector for initial content to land in the bucket.

6. Select the content check box and click the three dots on the right to download, extract, and view the file.

7. User your preferred log or text viewer to verify the content.