

Integrating Splunk Enterprise with Object Storage for Log Analytics

Exactly a year ago today (8/12/19) Splunk released a plugin that connects to Oracle Cloud's Object Storage. The purpose behind it is to allow users of both services to monitor logs collected in OCI.



Currently, there are five different types of logs that can be collected:

- Functions
- Object Storage
- Load Balancer Service
- Events Service
- Flow Logs


In my environment, I selected my VCN (Virtual Cloud Network) Logs to monitor my network traffic. I'll have the steps written below along with some links. Additionally, I'll add some screenshots of how it looks when configuring the plugin.

Sidenote: Originally, I downloaded the plugin through the Splunk App Dashboard. To make a long story short, there was an error I was running into when attempting to add the data. I contacted the original author of the Oracle blog and during a Zoom session we discovered a bug with the version of python that was bundled with it. Due to this it is only available through the website as a download while a solution is developed. I am using the Python 2.7 version of the plugin.

Prerequisites

- Logs
- Bucket in Object Storage for Logs
- Bucket's Namespace (Located in Bucket Information)
- Administrator Status on Splunk
- Secret and Access Keys (Follow the instructions [here](#))

How to enable logs in OCI

- 1) Click  the icon on the top left of the main OCI Dashboard
- 2) Scroll down to **Solutions and Platform** and select **Logging**
- 3) **Enable Log**
- 4) Select **Compartment, Service, Resource, Log Category** and name your Log
- 5) You can then create a **Log Group** and monitor all three Availability Domains in your VCN
- 6) Check Object Storage after some time to make sure the bucket was created. You can then edit retention policies etc.

Object Storage Plugin Installation & Configuration

- 1) Go to [Splunkbase](#) and download the plugin. (1.0.1 for python2.7 or 1.10 for python3.7)
- 2) On your Splunk Dashboard, click the gear icon next to **Apps**
- 3) Click **Install App from File** and upload the tgz file.
- 4) Restart the app and verify that it was installed properly by either clicking the gear icon again or by clicking **Splunk Apps** on the main menu then **Apps** at the top left then selecting **Manage Apps**.
- 5) To configure simply click **Settings** then **Data Inputs**
- 6) You'll see OCI Object Storage
- 7) Click **New**

Configuration Settings

- **Resource Name:** Your bucket name
- **Access Key:** Link to how to create is in the prerequisite section
- **Secret Key:** Link to how to create is in the prerequisite section
- **Endpoint:** *mynamespace.compat.objectstorage.us-phoenix-1.oraclecloud.com*
- **Region:** The region where your bucket is located. Ex: us-phoenix-1
- **Source Type:** Can be manually configured but if left on automatic Splunk will classify and assign the source type and give unknown's a placeholder name automatically

At this point you are done and simply need to wait for the logs to ingest into Splunk at which point you can create analyze your data and create custom dashboards

References

- Blog post about [Logging Services on OCI](#)
- Original post announcing the [Object Storage Plugin](#)

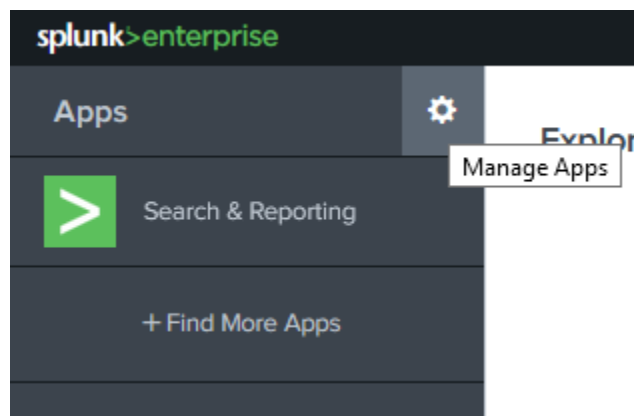
The following screenshots are in order and begin on the next page

Installing and Configuring the Object Storage Plugin App

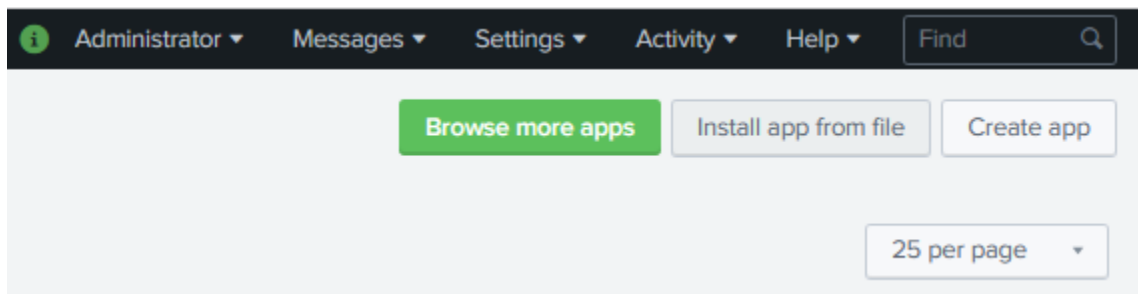
Step 1

The screenshot shows the 'Overview' tab of the Splunk App Store for the 'Splunk Add-on for Oracle Cloud Infrastructure (OCI) Object Storage'. The page includes a description, built-in source types (VCN Flow Logs, Load Balancer Logs, Audit Logs), and release notes for version 1.0.1 (Aug 8, 2020). On the right, there are statistics for 24 installs and 143 downloads, a 'Download' button, and a 'Rate this App' button. A version dropdown menu is open, showing options 1.0.1, 1.0.1, and 1.1.0. Below the version dropdown, there is a 'SUPPORT' section with links for 'Not Supported', 'Questions on Splunk Answers', 'Flag as inappropriate', and 'App Contents: Inputs'.

Step 2




Step 3



Step 4

Home	launcher
learned	learned
legacy	legacy
oci_objectstorage	oci_objectstorage
sample data	sample_app
Search & Reporting	search
Splunk Datasets Add-On	splunk_datasets_addon

Step 5


Administrator ▾


Messages ▾

Settings ▾

Activity ▾

Help ▾

Find


Add Data

KNOWLEDGE

[Searches, reports, and alerts](#)

[Data models](#)

[Event types](#)

[Tags](#)

[Fields](#)

[Lookups](#)

DATA

[Data inputs](#)

[Forwarding and receiving](#)

[Indexes](#)

[Report acceleration summaries](#)

[Virtual indexes](#)

[Source types](#)

Step 6

Scripts Run custom scripts to collect or generate more data.	5	+ Add new
OCI Object Storage Get data from S3 compliant OCI Object Storage.	1	+ Add new
Showing 1-1 of 1 modular inputs		

Step7

Source

Resource name *

A S3 resource name without the leading s3://. For example, for s3://bucket/file.txt specify bucket/file.txt. You can also monitor a whole bucket (for example by specifying 'bucket'), or files within a sub-directory of a bucket (for example 'bucket/some/directory/'; note the trailing slash).

Key ID *

Your Access key ID.

Secret key *

Your Secret key.

Endpoint *

mynamespace.compat.objectstorage.us-phoenix-1.oraclecloud.com

Region *

us-phoenix-1

Source type

Tell Splunk what kind of data this is so you can group it with other data of the same type when you search. Splunk does this automatically, but you can specify what you want if Splunk gets it wrong.

Set the source type

When this is set to automatic, Splunk classifies and assigns the sourcetype automatically, and gives unknown sourcetypes placeholder names.

More settings ☐

You're finished!!!