A Quick Start Guide to uploadSample: Uploading Sample Logs and Exploring Log Analytics

Last updated on January 10, 2018

This document provides instructions for using the uploadSample package to populate your Log Analytics Cloud Service trial or subscription with sample logs, and it serves a guide for exploring Log Analytics features quickly. This document, however, is not intended to be a tutorial on using Log Analytics.

Contents

Deploying uploadSample

This section documents how to ensure that the prerequisites of the uploadSample package are met, what the package contains, and how to install it.

Meeting the Prerequisites

Before using the uploadSample package to load sample logs to Log Analytics, ensure that the following prerequisites are met:

- You have a trial or subscription to Log Analytics cloud service

  > Note:
  > During the process of Log Analytics cloud service registration, you should receive an email notification from Oracle Cloud containing the information necessary for using this package including **Service Instance URL** and **Identity Domain**.

- You have access to a Unix variant host with cURL, which supports TLS 1.2 protocol
  - Checking TLS 1.2 support

    To check whether your cURL supports TLS 1.2 protocol, run the following command.

    ```
    $ curl --help | grep -i tlsv1.2
        --tlsv1.2        Use TLSv1.2 (SSL)
    ```

    If you see tls1.2 in the output, then it indicates that cURL supports TLS1.2 protocol.

  > Note:
  > This package cannot be implemented on a Windows platform.

- You have HTTPS connectivity from host to the Oracle Management Cloud (OMC)

  > Note:
  > If it is necessary to access Oracle Management Cloud through a proxy server, set the HTTPS_PROXY environment variable before running the cURL command.
  > Example:
  > `$ export HTTPS_PROXY=www-proxy.xyz.com:80`

  - Checking connectivity to OMC

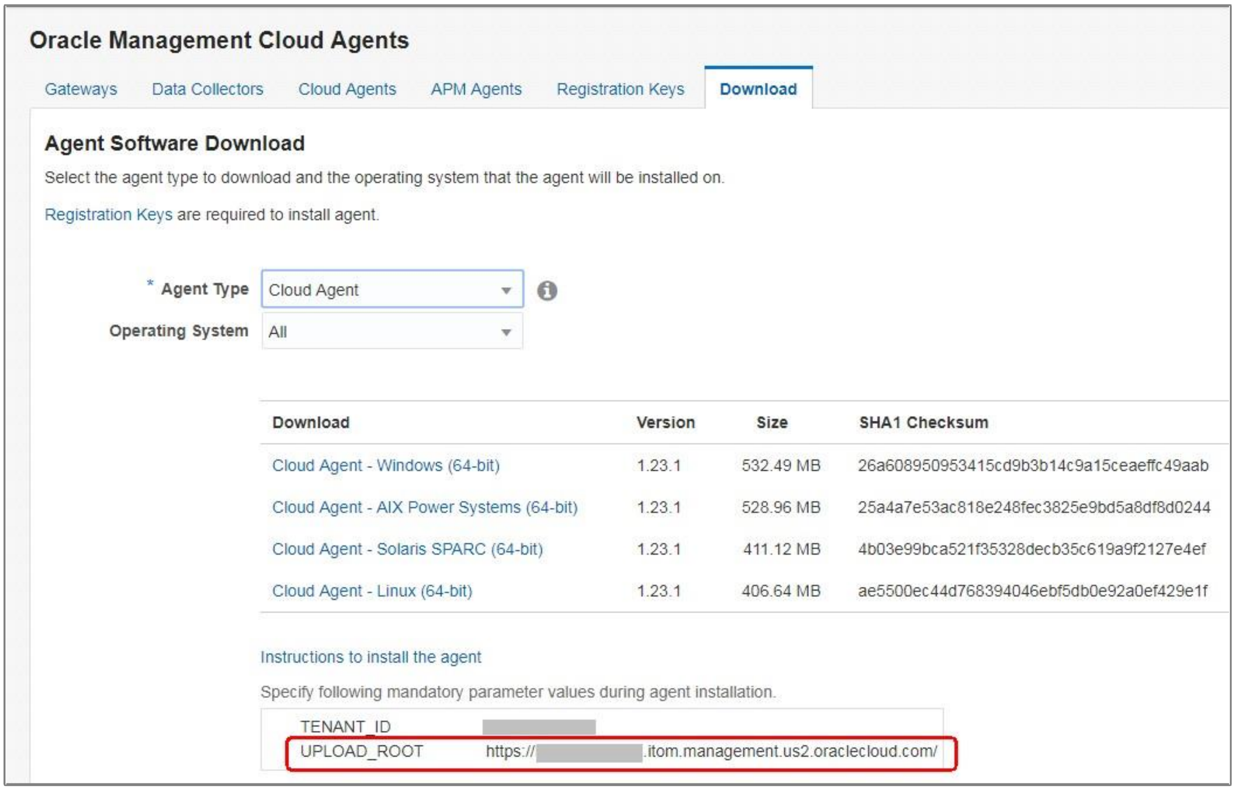
    Run the following command:

    ```
    $ curl -I --tlsv1.2 <UPLOAD_ROOT>
    ```

    <UPLOAD_ROOT>: URL for uploading logs to OMC

Note:
To obtain the value of the UPLOAD_ROOT parameter, log on to Oracle Management Cloud, navigate to **Administration**[*] > **Agents** > **Download** tab, and select an agent type from the **Agent Type** drop-down list. You should see the value of UPLOAD_ROOT at the bottom of the page as shown in the screenshot below.

[*] Click the navigation icon ☰ on the top-left corner to view the Management Cloud navigation pane if it is not already there.



Oracle Management Cloud Agents

Agent Software Download

Select the agent type to download and the operating system that the agent will be installed on.

Registration Keys are required to install agent.

* Agent Type: Cloud Agent

Operating System: All

Download	Version	Size	SHA1 Checksum
Cloud Agent - Windows (64-bit)	1.23.1	532.49 MB	26a608950953415cd9b3b14c9a15ceaeffc49aab
Cloud Agent - AIX Power Systems (64-bit)	1.23.1	528.96 MB	25a4a7e53ac818e248fec3825e9bd5a8df8d0244
Cloud Agent - Solaris SPARC (64-bit)	1.23.1	411.12 MB	4b03e99bca521f35328decb35c619a9f2127e4ef
Cloud Agent - Linux (64-bit)	1.23.1	406.64 MB	ae5500ec44d768394046ebf5db0e92a0ef429e1f

Instructions to install the agent

Specify following mandatory parameter values during agent installation.

TENANT_ID	[redacted]
UPLOAD_ROOT	https://[redacted].itom.management.us2.oraclecloud.com/

Example:

```
$ curl -I --tlsv1.2 https://inst1-acme.itom.management.us2.oraclecloud.com
```

If the command is successful, you will see an output similar to the one below.

```
HTTP/1.0 200 Connection established

HTTP/1.1 200 OK
Date: Sat, 19 Aug 2017 00:56:42 GMT
Server: Oracle-Application-Server-11g
X-Frame-Options: SAMEORIGIN
Last-Modified: Wed, 09 Dec 2015 23:27:01 GMT
ETag: "2b14-5267f6d5bfb40"
Accept-Ranges: bytes
Content-Length: 11028
Vary: Accept-Encoding
Cache-Control: no-cache,no-store
```

```
Content-Type: text/html
Content-Language: en
```

Contents of Package: uploadSample

The uploadSample package contains the following:

- uploadSample.sh: The shell script for uploading on demand the sample logs provided with the package
- uploadSampleTraditional.sh: Same as uploadSample.sh, except it is intended for Oracle Management Cloud tenant accounts using “Traditional Cloud Service” authentication.
- upload.properties: The file containing the properties used for uploading files
- Sample log files:
  - alertlog.zip containing sample database alert logs
  - messages.zip containing sample Linux syslog (system logs)
- uploadSample.pdf: The document you are reading

Installing uploadSample

To install the uploadSample package, follow these steps:

1. Download the uploadSample.zip file.
2. Stage the Zip file in a directory that your OS user account has read and write access. For example, stage the file in the /scratch directory.
3. Go to the stage directory and unzip the file.

   Example:

   ```
   $ cd /scratch
   $ unzip uploadSample.zip
   ```

   After extracting the Zip file as above, you will see a subdirectory named uploadSample in the current directory. This document refers to the uploadSample directory as SCRIPT_HOME.

Using uploadSample

The section provides the steps for using the uploadSample package to upload sample logs to explore Log Analytics features.

Uploading Sample Logs to Log Analytics

To upload the provided sample logs, follow these steps:

1. Before uploading logs, enter properties' values to be used in uploading logs in file <SCRIPT_HOME>/config/ upload.properties.
   - Go to the <SCRIPT_HOME>/config directory.

     > Note:
     > If you extracted file uploadSample.zip to directory /scratch, directory /scratch/uploadSample is your SCRIPT_HOME directory.

   - Use an editor of your choice to edit file upload.properties to set appropriate values for the following properties:

     Mandatory properties:

     ```
     UPLOAD_ROOT=<URL for uploading data to Oracle Management Cloud>
     Examples:
     UPLOAD_ROOT=https://inst1-acme.itom.management.us2.oraclecloud.com
     UPLOAD_ROOT=https://inst1-xyz.itom.management.europe.oraclecloud.com
     UPLOAD_ROOT=https://a123456.itom.management.us2.oraclecloud.com

     IDENTITY_DOMAIN=<Subscription identity domain>
     Example:
     IDENTITY_DOMAIN=acme

     USERNAME=<OMC user name>
     Example:
     USERNAME=john.doe@xyz.com
     ```

     Optional property:

     ```
     HTTPS_PROXY=<proxy_host>:<port>
     Example:
     HTTPS_PROXY=www-proxy.xyz.com:80
     ```

     > Note:
     > For obtaining the value of property UPLOAD_ROOT, see Meeting the Prerequisites.

2. Go to the SCRIPT_HOME directory, and run the uploadSample.sh script to upload the sample alert logs and syslog, respectively, as shown below. Enter your OMC password when prompted.

```
$ ./uploadSample.sh alertlog
$ ./uploadSample.sh syslog
```

Note:

If your tenant uses Traditional Cloud Account for authentication (most likely because your tenant was created prior to April 2018), use uploadSampleTraditional.sh instead.

Take note of the name of the upload at the bottom of each script output. An upload is identified by its name in Log Analytics UI.

Examples of output lines containing upload names are:

```
Upload name: alertlog.2018-01-07_19:43:25
Upload name: syslog.2018-01-07_19:43:32
```

Note:

The uploadSample.sh will create the following entities, if they do not exist, when uploading logs:

- **demo_db_instance**: when uploading alert logs
- **demo_host**: when uploading syslog

In Log Analytics, you can query log records based on fields such as entity and upload name.

Verifying the Status of Uploads

To verify the status of the uploads, follow these steps:

1. Log on to Oracle Management Cloud
   - Go to the Service Instance URL.

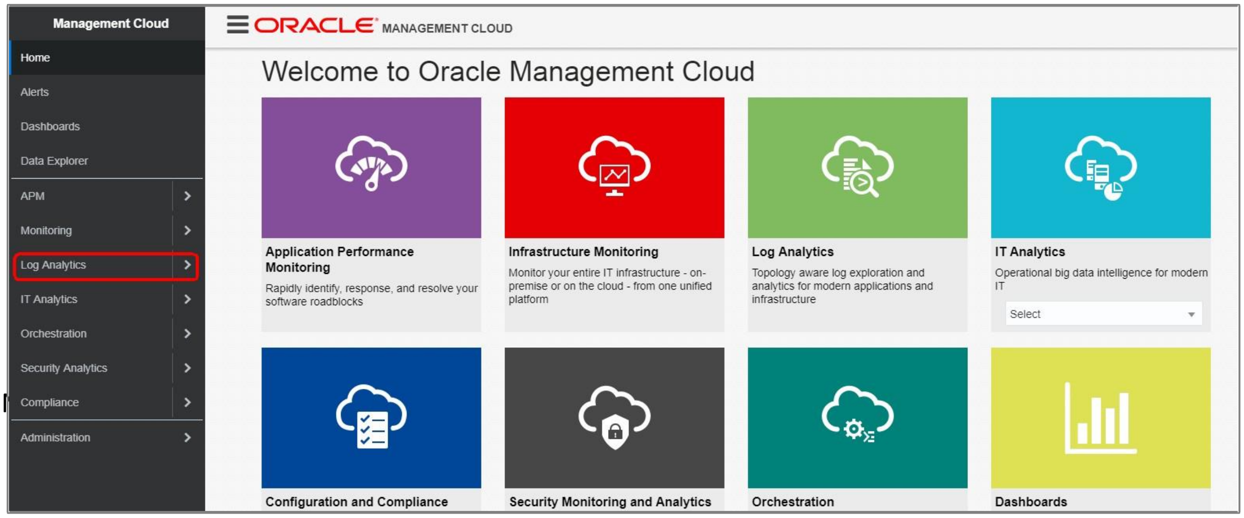
     Note:

     After a user account is created for you, you will receive an email titled “You’re the administrator for Oracle Cloud Services” from Oracle Cloud, which contains the Service Instance URL.

   - Enter your identity domain, and click **Go**.
   - Enter your username and password, and click **Sign In**.

2. Navigate to Log Analytics

   From the Welcome to Oracle Management Cloud page, click the navigation icon ≡ on the top-left corner to view the Management Cloud navigation pane if it is not already there. Select **Log Analytics**.



Welcome to Oracle Management Cloud

Application Performance Monitoring
Rapidly identify, response, and resolve your software roadblocks

Infrastructure Monitoring
Monitor your entire IT infrastructure - on-premise or on the cloud - from one unified platform

Log Analytics
Topology aware log exploration and analytics for modern applications and infrastructure

IT Analytics
Operational big data intelligence for modern IT

Configuration and Compliance

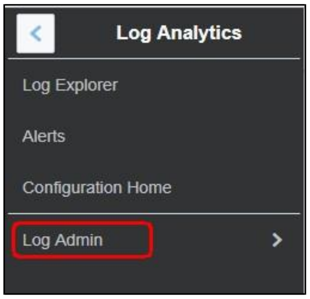
Security Monitoring and Analytics

Orchestration

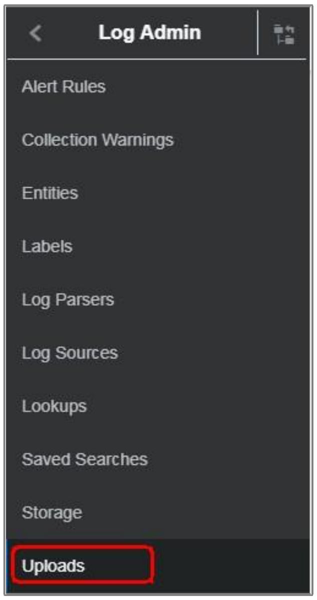
Dashboards

3. l

a. From the left navigation pane, select **Log Admin**.

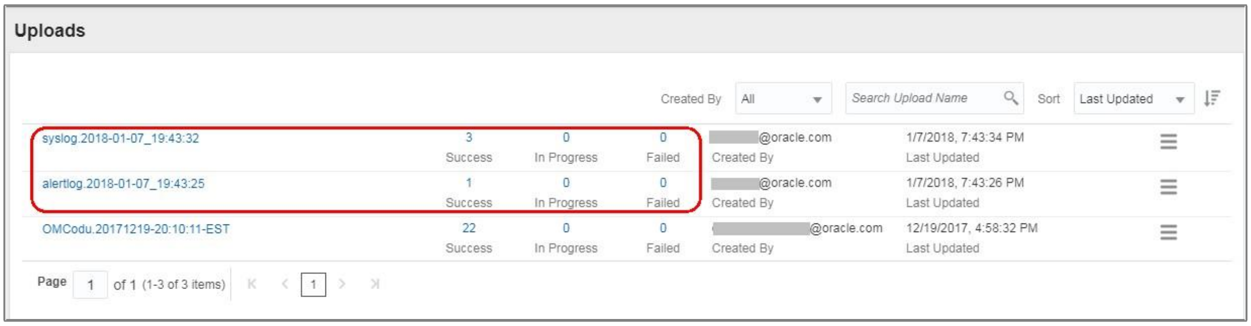


b. Select **Uploads**.



4. View the status of the uploads

From the Uploads page, you should see the uploads that you performed earlier. If an upload shows 0 in Progress and 0 Failed, it has completed.



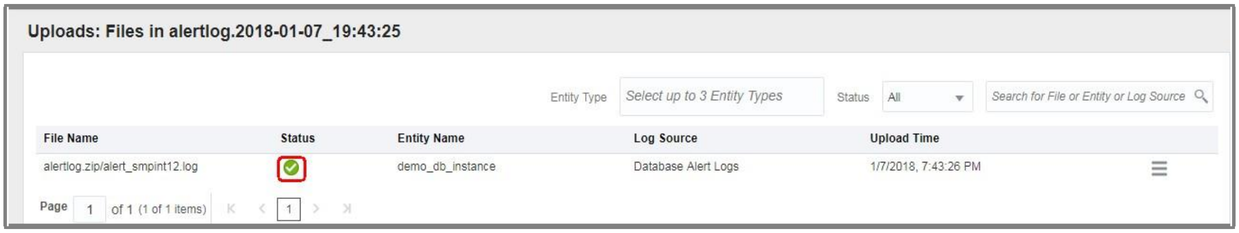
Uploads

Created By: All | Search Upload Name | Sort: Last Updated

syslog.2018-01-07_19:43:32	3 Success	0 In Progress	0 Failed	[redacted]@oracle.com Created By	1/7/2018, 7:43:34 PM Last Updated
alertlog.2018-01-07_19:43:25	1 Success	0 In Progress	0 Failed	[redacted]@oracle.com Created By	1/7/2018, 7:43:26 PM Last Updated
OMCodu.20171219-20:10:11-EST	22 Success	0 In Progress	0 Failed	[redacted]@oracle.com Created By	12/19/2017, 4:58:32 PM Last Updated

Page 1 of 1 (1-3 of 3 items)

If necessary, click an upload name to see the Status of the upload. For example, click **alertlog_<timestamp>**. If the upload has completed successfully, you will seen a green stick in the Status field as shown in the screenshot below.



Uploads: Files in alertlog.2018-01-07_19:43:25

Entity Type
Select up to 3 Entity Types
Status
All
Search for File or Entity or Log Source

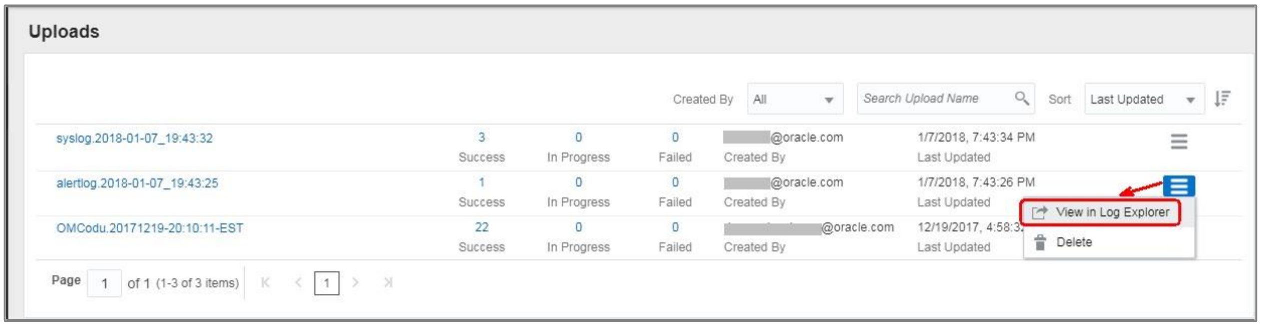
File Name	Status	Entity Name	Log Source	Upload Time
alertlog.zip/alert_smpint12.log	✓	demo_db_instance	Database Alert Logs	1/7/2018, 7:43:26 PM

Page 1 of 1 (1 of 1 items)
1

Viewing Uploaded Log Records

To view the records from an upload, follow these steps:

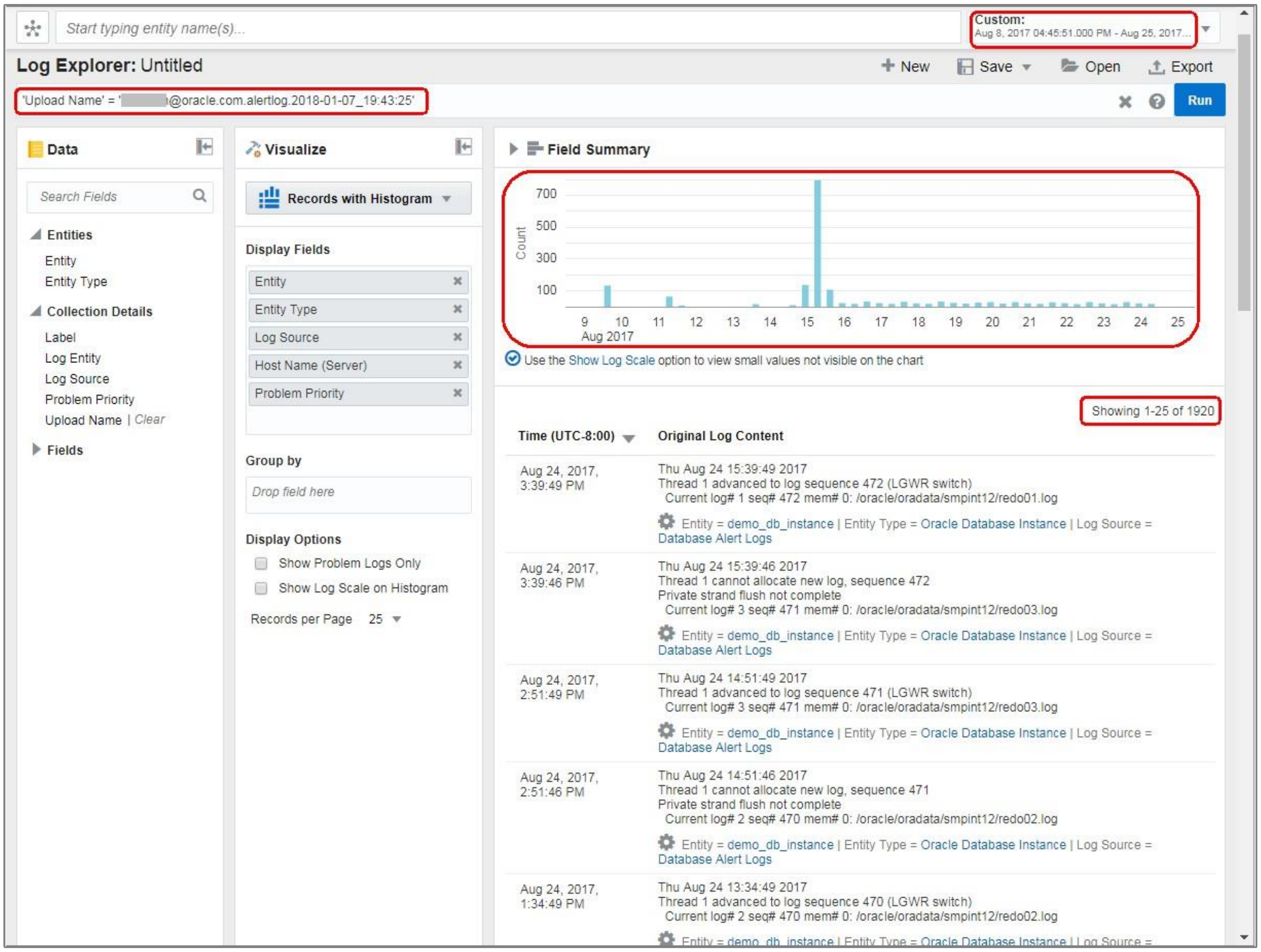
1. Navigate to the Uploads page. If necessary, see Verifying the Statuses of Uploads.
2. From the Uploads page, select an upload, click the menu icon ☰ on the right, and click **View in Log Explorer** to view the records from that upload. Let's perform the steps to view the alert log records in Log Explorer.



Uploads

syslog.2018-01-07_19:43:32	3 Success	0 In Progress	0 Failed	[redacted]@oracle.com Created By	1/7/2018, 7:43:34 PM Last Updated
alertlog.2018-01-07_19:43:25	1 Success	0 In Progress	0 Failed	[redacted]@oracle.com Created By	1/7/2018, 7:43:26 PM Last Updated
OMCodu.20171219-20:10:11-EST	22 Success	0 In Progress	0 Failed	[redacted]@oracle.com Created By	12/19/2017, 4:58:3 Last Updated

3. From the Log Explorer page, you can view the alert log records from the upload that you selected.



Custom:
Aug 8, 2017 04:45:51.000 PM - Aug 25, 2017...

'Upload Name' = '[redacted]@oracle.com.alertlog.2018-01-07_19:43:25'

Display Fields: Entity, Entity Type, Log Source, Host Name (Server), Problem Priority

□ Show Problem Logs Only
□ Show Log Scale on Histogram
Records per Page 25

Use the Show Log Scale option to view small values not visible on the chart

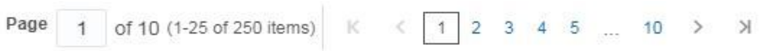
Showing 1-25 of 1920

```
Aug 24, 2017,   Thu Aug 24 15:39:49 2017
3:39:49 PM      Thread 1 advanced to log sequence 472 (LGWR switch)
                  Current log# 1 seq# 472 mem# 0: /oracle/oradata/smpint12/redo01.log
                Entity = demo_db_instance | Entity Type = Oracle Database Instance | Log Source =
                Database Alert Logs

Aug 24, 2017,   Thu Aug 24 15:39:46 2017
3:39:46 PM      Thread 1 cannot allocate new log, sequence 472
                Private strand flush not complete
                  Current log# 3 seq# 471 mem# 0: /oracle/oradata/smpint12/redo03.log
                Entity = demo_db_instance | Entity Type = Oracle Database Instance | Log Source =
                Database Alert Logs

Aug 24, 2017,   Thu Aug 24 14:51:49 2017
2:51:49 PM      Thread 1 advanced to log sequence 471 (LGWR switch)
                  Current log# 3 seq# 471 mem# 0: /oracle/oradata/smpint12/redo03.log
                Entity = demo_db_instance | Entity Type = Oracle Database Instance | Log Source =
                Database Alert Logs

Aug 24, 2017,   Thu Aug 24 14:51:46 2017
2:51:46 PM      Thread 1 cannot allocate new log, sequence 471
                Private strand flush not complete
                  Current log# 2 seq# 470 mem# 0: /oracle/oradata/smpint12/redo02.log
                Entity = demo_db_instance | Entity Type = Oracle Database Instance | Log Source =
                Database Alert Logs

Aug 24, 2017,   Thu Aug 24 13:34:49 2017
1:34:49 PM      Thread 1 advanced to log sequence 470 (LGWR switch)
                  Current log# 2 seq# 470 mem# 0: /oracle/oradata/smpint12/redo02.log
                Entity = demo_db_instance | Entity Type = Oracle Database Instance | Log Source =
```

Some of the information shown on the page includes:

- The uploaded alert log entries are for the period from August 9 to August 24, 2017.
- The log entries came from the upload whose name is in the Query bar.
- The histogram shows the daily volumes of log records. This helps identify any abnormality in record volumes at a glance. You can drill down by clicking a bar on the chart.
- The first 25 of the 1920 records that came with the upload. The records are in date order from newest to oldest. You can reverse the order by clicking the arrowhead in the Time (<time zone>) field.

  You can browse the rest of log records by using the pagination at the bottom of the page.

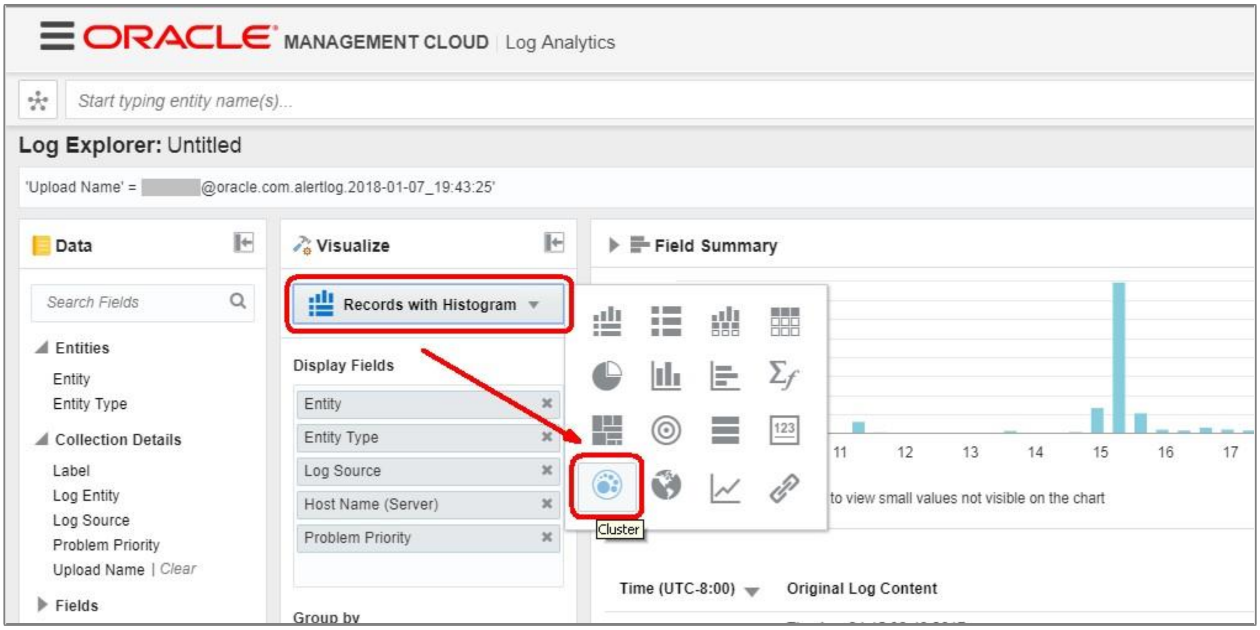

Page 1 of 10 (1-25 of 250 items)

Detecting Anomalies with Cluster Command

To detect anomalies based on log records, you can use Log Analytics cluster command, which automatically groups log records based on severity, such as error, fault, fatal and warning, and dynamically identified patterns, potential issues, outliers, and trends.

- Clustering Logs

To perform clustering on the log records, from the **Visualize** panel click the currently selected visualization (e.g. **Records with Histogram**), and click **Cluster** icon ⦿.

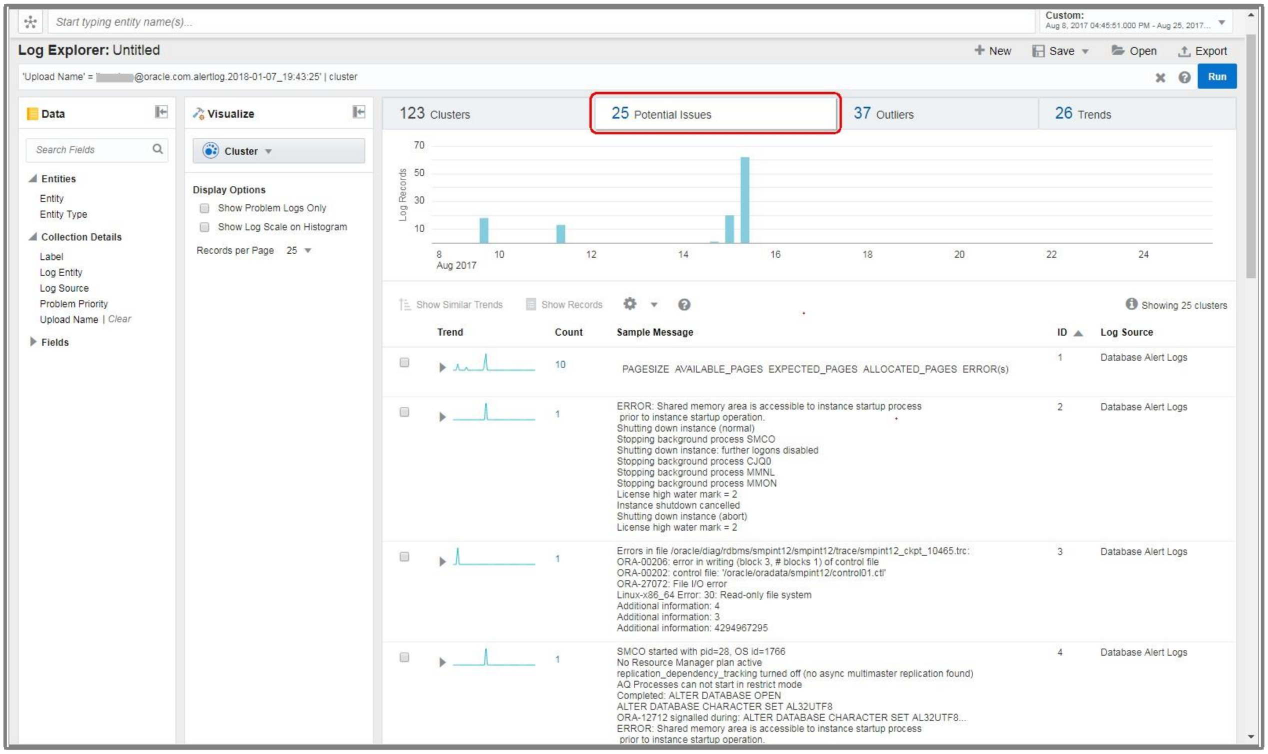

ORACLE MANAGEMENT CLOUD | Log Analytics
Start typing entity name(s)...
Log Explorer: Untitled

'Upload Name' = [redacted]@oracle.com.alertlog.2018-01-07_19:43:25'

- Checking the Outcome of the Cluster Operation

The cluster operation reduced 1920 log records to 123 clusters, identified 25 potential issues, 37 outliers, and 26 trends.

Examine the log clusters, and then click **Potential Issues**.


Start typing entity name(s)...
Custom:
Aug 8, 2017 04:45:51.000 PM - Aug 25, 2017...
Log Explorer: Untitled
New
Save
Open
Export
Run

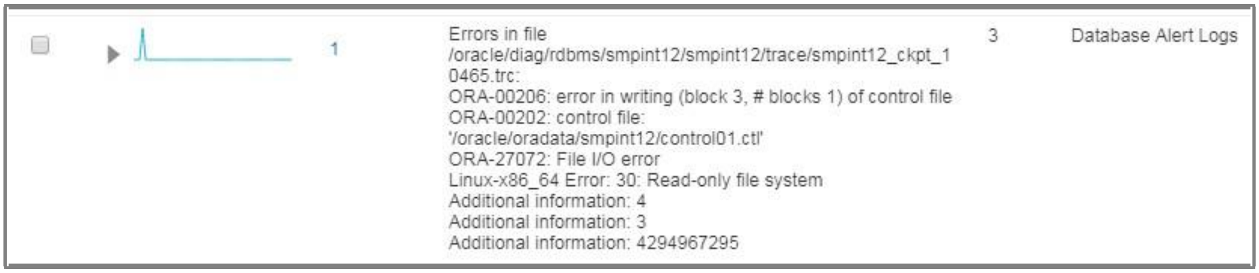
'Upload Name' = [redacted]@oracle.com.alertlog.2018-01-07_19:43:25' | cluster

	Trend	Count	Sample Message	ID ▲	Log Source
□	▶	10	PAGESIZE AVAILABLE_PAGES EXPECTED_PAGES ALLOCATED_PAGES ERROR(s)	1	Database Alert Logs
□	▶	1	ERROR: Shared memory area is accessible to instance startup process prior to instance startup operation. Shutting down instance (normal) Stopping background process SMCO Shutting down instance: further logons disabled Stopping background process CJQ0 Stopping background process MMNL Stopping background process MMON License high water mark = 2 Instance shutdown cancelled Shutting down instance (abort) License high water mark = 2	2	Database Alert Logs
□	▶	1	Errors in file /oracle/diag/rdbms/smpint12/smpint12/trace/smpint12_ckpt_10465.trc: ORA-00206: error in writing (block 3, # blocks 1) of control file ORA-00202: control file: '/oracle/oradata/smpint12/control01.ctl' ORA-27072: File I/O error Linux-x86_64 Error: 30: Read-only file system Additional information: 4 Additional information: 3 Additional information: 4294967295	3	Database Alert Logs
□	▶	1	SMCO started with pid=28, OS id=1766 No Resource Manager plan active replication_dependency_tracking turned off (no async multimaster replication found) AQ Processes can not start in restrict mode Completed: ALTER DATABASE OPEN ALTER DATABASE CHARACTER SET AL32UTF8 ORA-12712 signalled during: ALTER DATABASE CHARACTER SET AL32UTF8... ERROR: Shared memory area is accessible to instance startup process prior to instance startup operation.	4	Database Alert Logs

- Examining Potential Issues

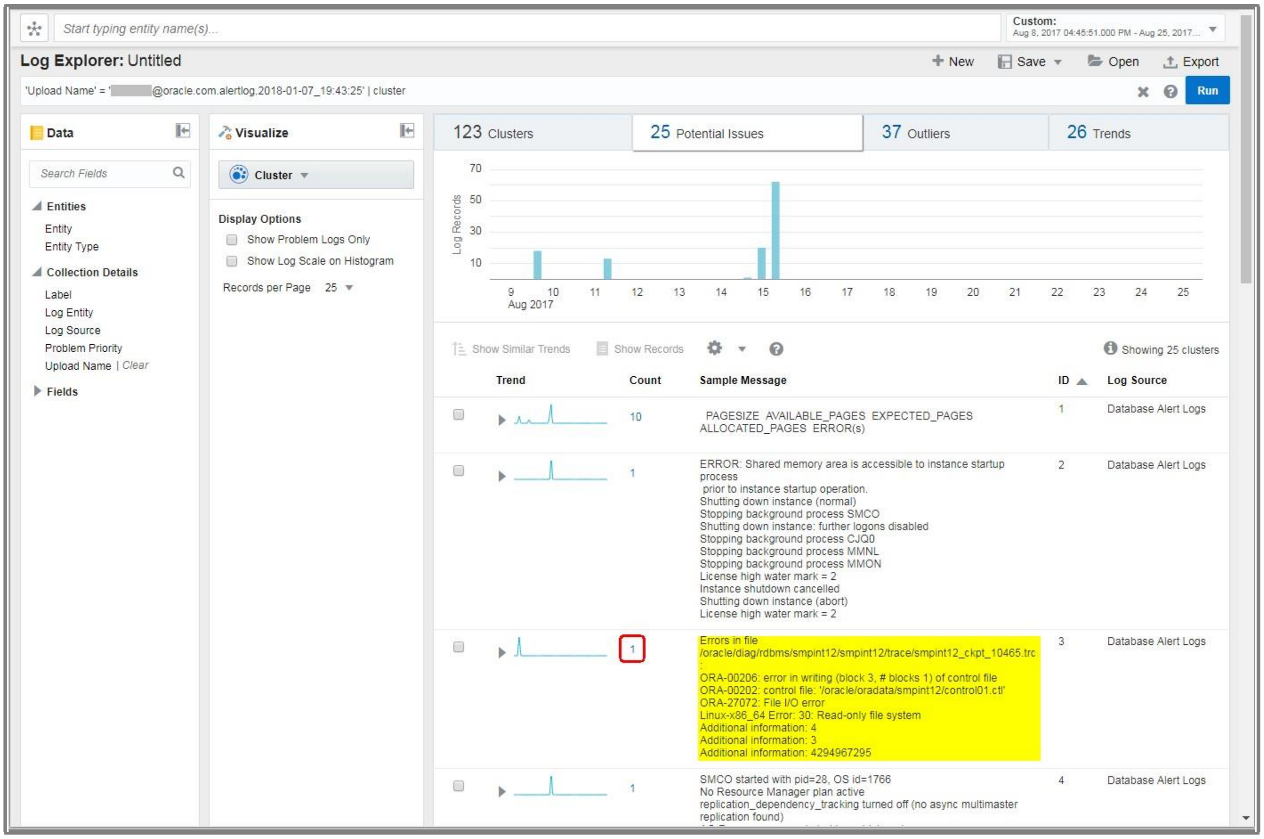
From the **Potential Issues** tab, you can look at the log clusters that Log Analytics identifies as potential issues, if you see a cluster with a sample message that may be pointing to an issue of significance or of interest, click the value in the **Count** column to drill down see the records of the cluster.

For example, the following sample message indicates that the Oracle database instance had problems writing to a control file due to a file I/O error. This kind of problem is critical; it tends to result in an abnormal shutdown of the instance.



□	▶	1	Errors in file /oracle/diag/rdbms/smpint12/smpint12/trace/smpint12_ckpt_10465.trc: ORA-00206: error in writing (block 3, # blocks 1) of control file ORA-00202: control file: '/oracle/oradata/smpint12/control01.ctl' ORA-27072: File I/O error Linux-x86_64 Error: 30: Read-only file system Additional information: 4 Additional information: 3 Additional information: 4294967295	3	Database Alert Logs

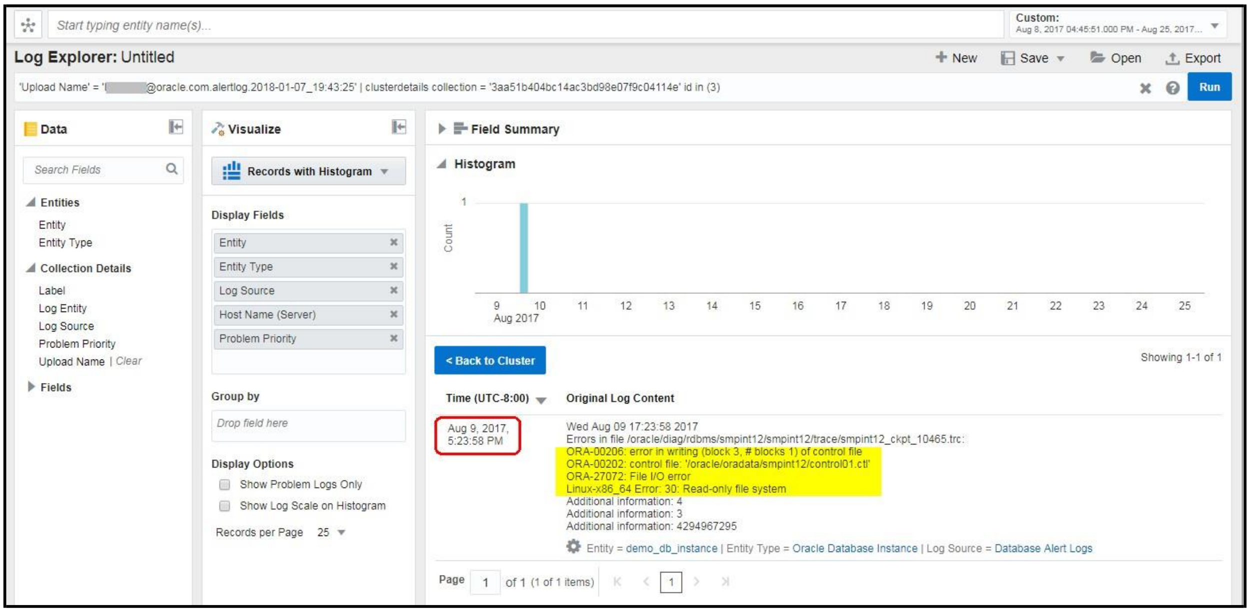
Let’s drill down to the log record by clicking the count value of 1 on the left of the sample message.



'Upload Name' = '[redacted]@oracle.com.alertlog.2018-01-07_19:43:25' | cluster

	Trend	Count	Sample Message	ID	Log Source
□	▶	10	PAGESIZE AVAILABLE_PAGES EXPECTED_PAGES ALLOCATED_PAGES ERROR(s)	1	Database Alert Logs
□	▶	1	ERROR: Shared memory area is accessible to instance startup process prior to instance startup operation. Shutting down instance (normal) Stopping background process SMCO Shutting down instance: further logons disabled Stopping background process CJQ0 Stopping background process MMNL Stopping background process MMON License high water mark = 2 Instance shutdown cancelled Shutting down instance (abort) License high water mark = 2	2	Database Alert Logs
□	▶	1	Errors in file /oracle/diag/rdbms/smpint12/smpint12/trace/smpint12_ckpt_10465.trc : ORA-00206: error in writing (block 3, # blocks 1) of control file ORA-00202: control file: '/oracle/oradata/smpint12/control01.ctl' ORA-27072: File I/O error Linux-x86_64 Error: 30: Read-only file system Additional information: 4 Additional information: 3 Additional information: 4294967295	3	Database Alert Logs
□	▶	1	SMCO started with pid=28, OS id=1766 No Resource Manager plan active replication_dependency_tracking turned off (no async multimaster replication found)	4	Database Alert Logs

Drilling down on a log cluster allows you to see the log record(s) including the original log entry (or entries) in that cluster. In this case, you will see the record with the timestamp of Aug 9, 2017, 5:23:58PM (UTC-8:00 or PST) showing a file I/O error affecting the writing to a database control file.



Custom: Aug 8, 2017 04:45:51.000 PM - Aug 25, 2017...

Log Explorer: Untitled

```
'Upload Name' = '[redacted]@oracle.com.alertlog.2018-01-07_19:43:25' | clusterdetails collection = '3aa51b404bc14ac3bd98e07f9c04114e' id in (3)
```

Display Fields: Entity, Entity Type, Log Source, Host Name (Server), Problem Priority

Display Options: □ Show Problem Logs Only □ Show Log Scale on Histogram

Records per Page 25

Time (UTC-8:00)	Original Log Content
Aug 9, 2017, 5:23:58 PM	Wed Aug 09 17:23:58 2017 Errors in file /oracle/diag/rdbms/smpint12/smpint12/trace/smpint12_ckpt_10465.trc: ORA-00206: error in writing (block 3, # blocks 1) of control file ORA-00202: control file: '/oracle/oradata/smpint12/control01.ctl' ORA-27072: File I/O error Linux-x86_64 Error: 30: Read-only file system Additional information: 4 Additional information: 3 Additional information: 4294967295 Entity = demo_db_instance | Entity Type = Oracle Database Instance | Log Source = Database Alert Logs

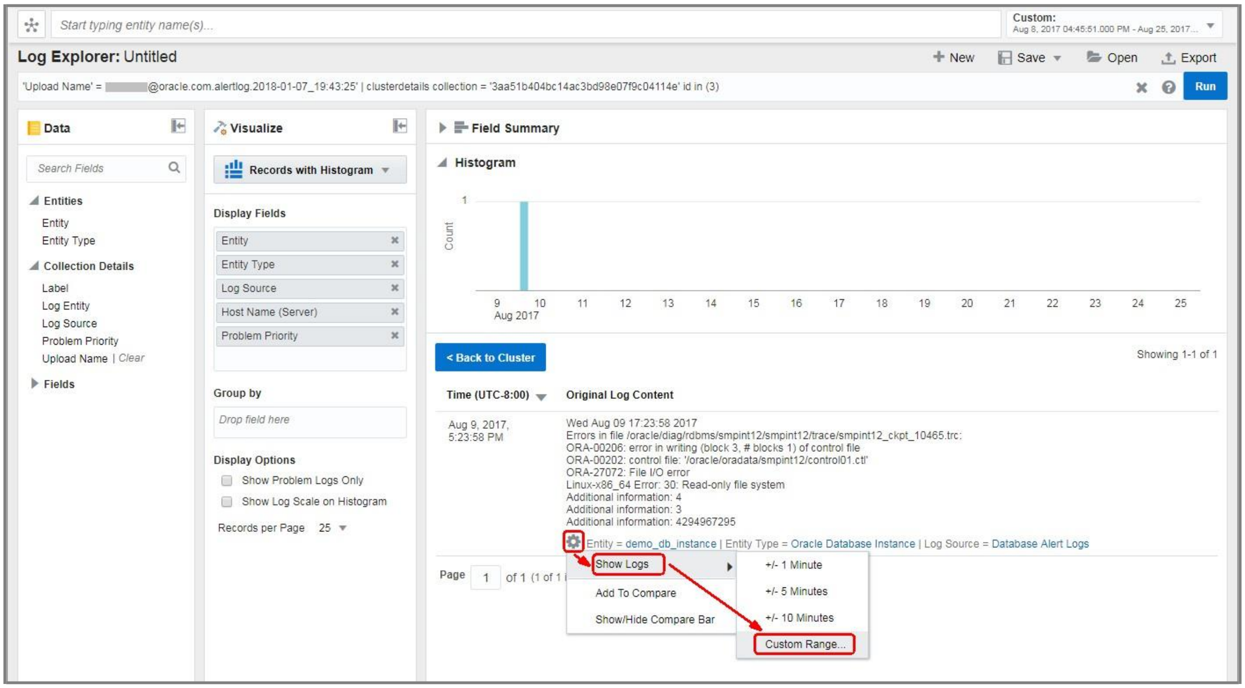
Showing 1-1 of 1

Page 1 of 1 (1 of 1 items)

Correlating Logs

Log Analytics allows you to quickly correlate logs from different sources (e.g. database logs and syslog) based on time to determine whether there is a correlation between events captured in log records. Let's query the log records for entities demo_db_instance and demo_host 30 seconds before 5:23:28 PM (UTC-8:00) and 30 seconds after that by following these steps:

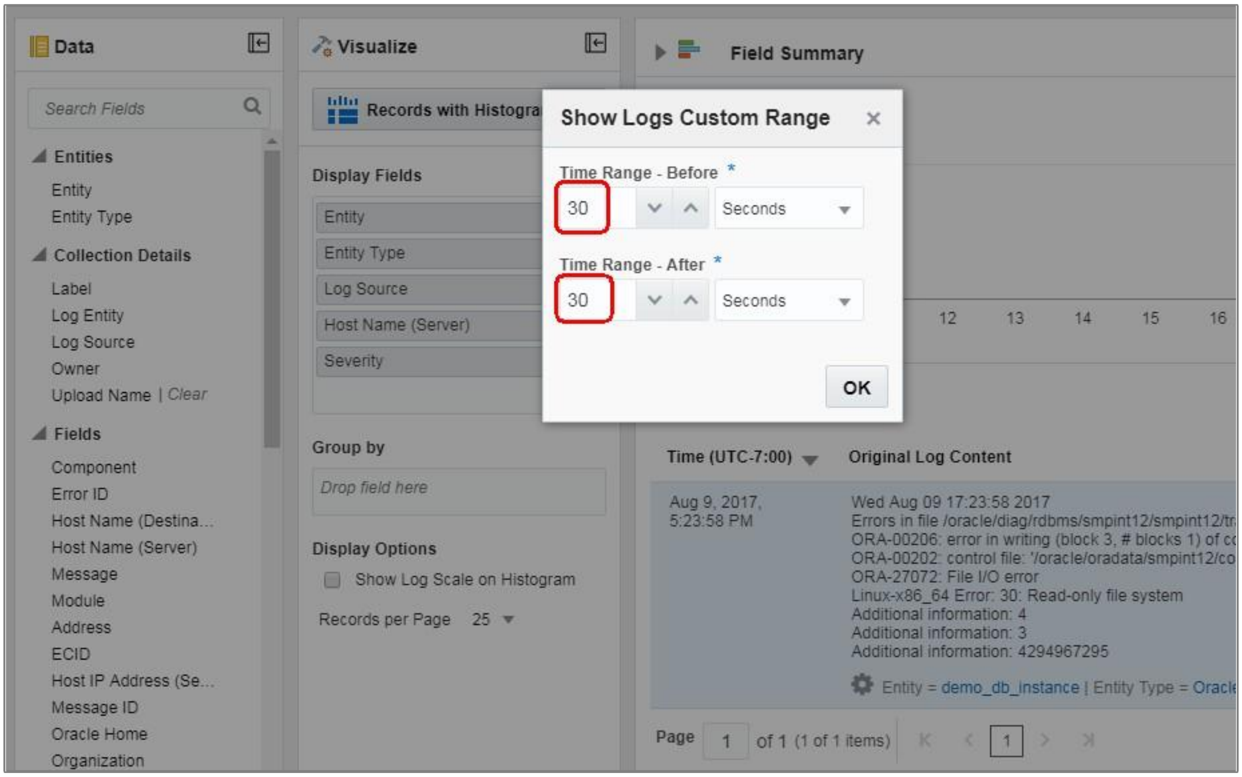
1. Click ⚙ at the bottom of the **Original Log Content** field, and then select **Show Logs**, **Custom Range**.



```
'Upload Name' = [redacted]@oracle.com.alertlog.2018-01-07_19:43:25' | clusterdetails collection = '3aa51b404bc14ac3bd98e07f9c04114e' id in (3)
```

Time (UTC-8:00)	Original Log Content
Aug 9, 2017, 5:23:58 PM	Wed Aug 09 17:23:58 2017 Errors in file /oracle/diag/rdbms/smpint12/smpint12/trace/smpint12_ckpt_10465.trc: ORA-00206: error in writing (block 3, # blocks 1) of control file ORA-00202: control file: '/oracle/oradata/smpint12/control01.ctl' ORA-27072: File I/O error Linux-x86_64 Error: 30: Read-only file system Additional information: 4 Additional information: 3 Additional information: 4294967295 Entity = demo_db_instance | Entity Type = Oracle Database Instance | Log Source = Database Alert Logs

2. From the Show Logs Custom Range pop-up window, enter 30 (seconds) for **Time Range - Before**, 30 (seconds) for **Time Range – After**, and click **OK**.



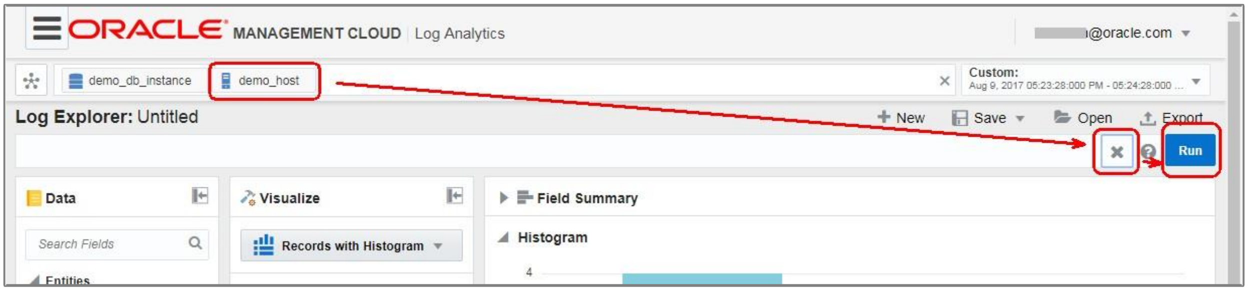
Show Logs Custom Range

Time Range - Before * 30 Seconds

Time Range - After * 30 Seconds

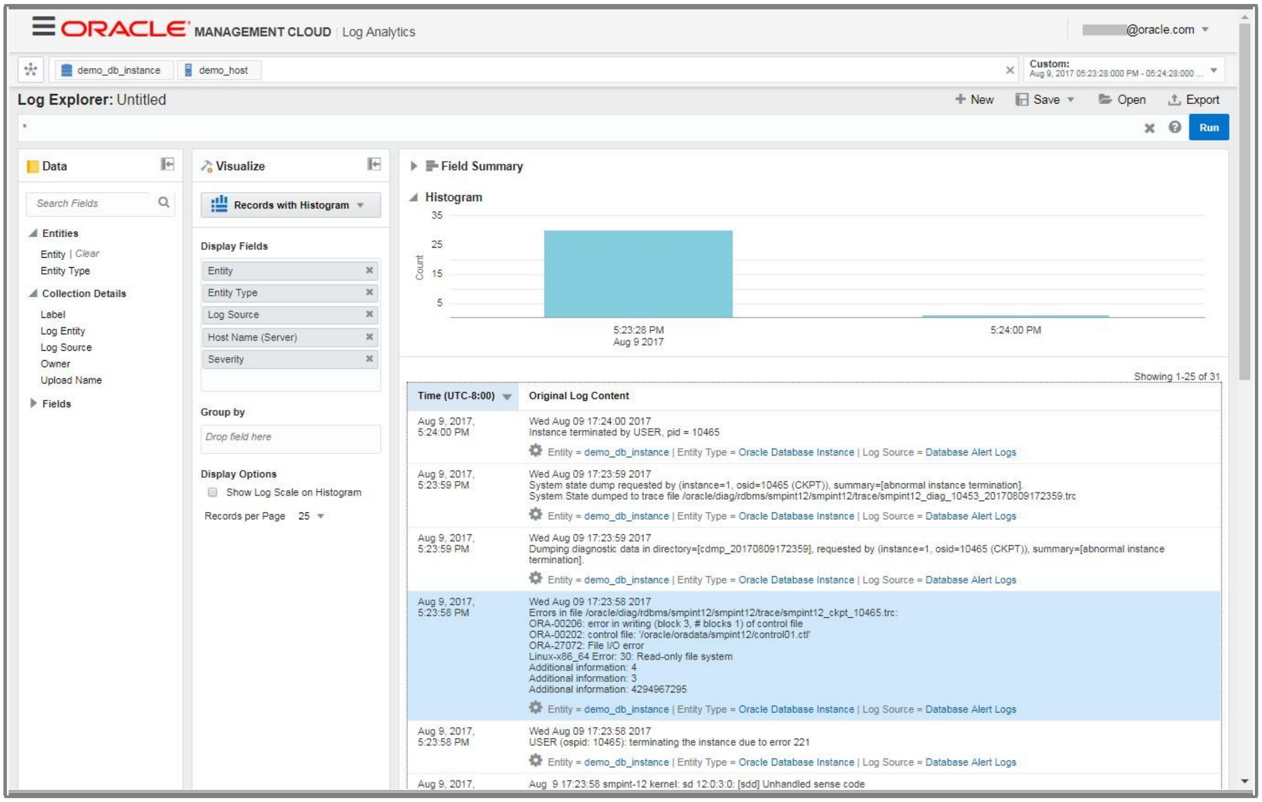
Time (UTC-7:00)	Original Log Content
Aug 9, 2017, 5:23:58 PM	Wed Aug 09 17:23:58 2017 Errors in file /oracle/diag/rdbms/smpint12/smpint12/tr ORA-00206: error in writing (block 3, # blocks 1) of c ORA-00202: control file: '/oracle/oradata/smpint12/co ORA-27072: File I/O error Linux-x86_64 Error: 30: Read-only file system Additional information: 4 Additional information: 3 Additional information: 4294967295 Entity = demo_db_instance | Entity Type = Oracl

3. In the Global Context ✱ bar near the top, enter demo_host next to demo_db_instance, click ✖ in the Query bar to clear any existing filter, and click **Run**.



Custom: Aug 9, 2017 05:23:28:000 PM - 05:24:28:000 ...

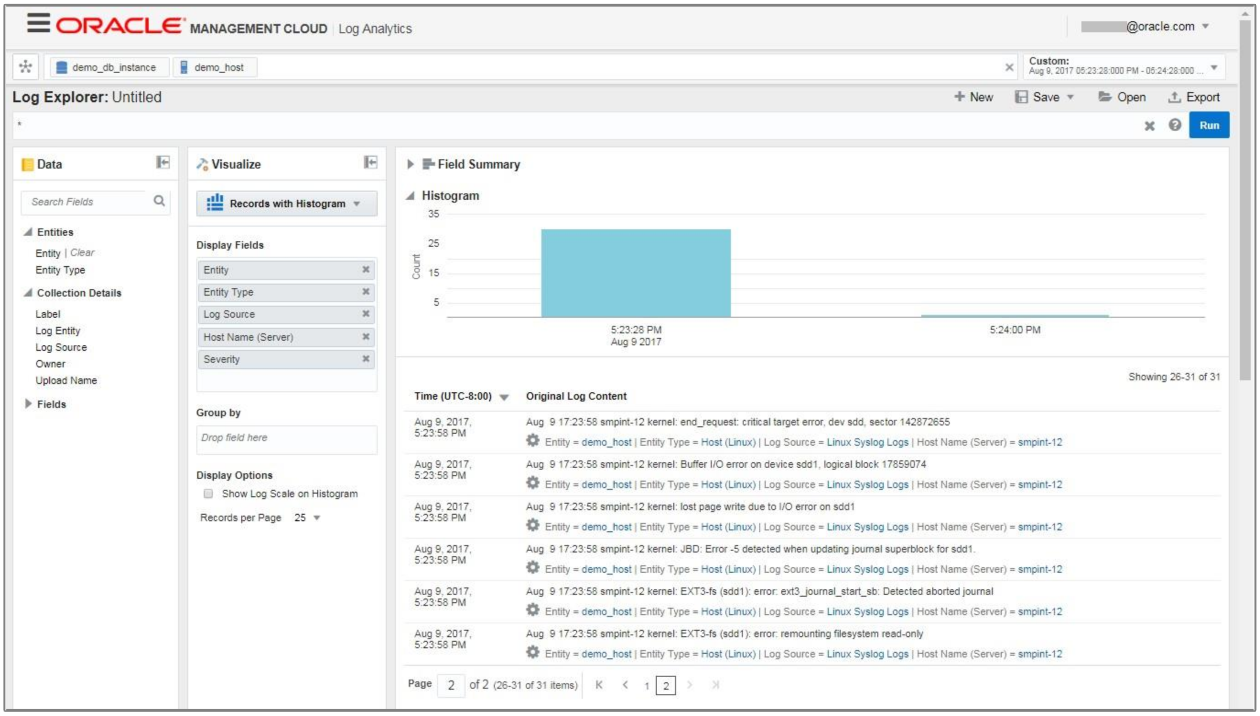
4. The above query retrieves the log records uploaded for entities demo_db_instance and demo_host for the period of 5:23:28 PM to 5:24:28 PM on August 9. Examine the 31 records in the two-page output to see the sequence of the events that were captured in the logs in the one-minute period, and which of the events may have had an effect on other events.



Custom: Aug 9, 2017 05:23:28:000 PM - 05:24:28:000 ...

Showing 1-25 of 31

Time (UTC-8:00)	Original Log Content
Aug 9, 2017, 5:24:00 PM	Wed Aug 09 17:24:00 2017 Instance terminated by USER, pid = 10465 Entity = demo_db_instance | Entity Type = Oracle Database Instance | Log Source = Database Alert Logs
Aug 9, 2017, 5:23:59 PM	Wed Aug 09 17:23:59 2017 System state dump requested by (instance=1, osid=10465 (CKPT)), summary=[abnormal instance termination]. System State dumped to trace file /oracle/diag/rdbms/smpint12/smpint12/trace/smpint12_diag_10453_20170809172359.trc Entity = demo_db_instance | Entity Type = Oracle Database Instance | Log Source = Database Alert Logs
Aug 9, 2017, 5:23:59 PM	Wed Aug 09 17:23:59 2017 Dumping diagnostic data in directory=[cdmp_20170809172359], requested by (instance=1, osid=10465 (CKPT)), summary=[abnormal instance termination]. Entity = demo_db_instance | Entity Type = Oracle Database Instance | Log Source = Database Alert Logs
Aug 9, 2017, 5:23:58 PM	Wed Aug 09 17:23:58 2017 Errors in file /oracle/diag/rdbms/smpint12/smpint12/trace/smpint12_ckpt_10465.trc: ORA-00206: error in writing (block 3, # blocks 1) of control file ORA-00202: control file: '/oracle/oradata/smpint12/control01.ctl' ORA-27072: File I/O error Linux-x86_64 Error: 30: Read-only file system Additional information: 4 Additional information: 3 Additional information: 4294967295 Entity = demo_db_instance | Entity Type = Oracle Database Instance | Log Source = Database Alert Logs
Aug 9, 2017, 5:23:58 PM	Wed Aug 09 17:23:58 2017 USER (ospid: 10465): terminating the instance due to error 221 Entity = demo_db_instance | Entity Type = Oracle Database Instance | Log Source = Database Alert Logs
Aug 9, 2017,	Aug 9 17:23:58 smpint-12 kernel: sd 12:0:3:0: [sdd] Unhandled sense code



Custom:
Aug 9, 2017 05:23:28:000 PM - 05:24:28:000 ...

*

Display Fields: Entity, Entity Type, Log Source, Host Name (Server), Severity

☐ Show Log Scale on Histogram

Records per Page 25

Showing 26-31 of 31

Time (UTC-8:00)	Original Log Content
Aug 9, 2017, 5:23:58 PM	Aug 9 17:23:58 smpint-12 kernel: end_request: critical target error, dev sdd, sector 142872655 Entity = demo_host | Entity Type = Host (Linux) | Log Source = Linux Syslog Logs | Host Name (Server) = smpint-12
Aug 9, 2017, 5:23:58 PM	Aug 9 17:23:58 smpint-12 kernel: Buffer I/O error on device sdd1, logical block 17859074 Entity = demo_host | Entity Type = Host (Linux) | Log Source = Linux Syslog Logs | Host Name (Server) = smpint-12
Aug 9, 2017, 5:23:58 PM	Aug 9 17:23:58 smpint-12 kernel: lost page write due to I/O error on sdd1 Entity = demo_host | Entity Type = Host (Linux) | Log Source = Linux Syslog Logs | Host Name (Server) = smpint-12
Aug 9, 2017, 5:23:58 PM	Aug 9 17:23:58 smpint-12 kernel: JBD: Error -5 detected when updating journal superblock for sdd1. Entity = demo_host | Entity Type = Host (Linux) | Log Source = Linux Syslog Logs | Host Name (Server) = smpint-12
Aug 9, 2017, 5:23:58 PM	Aug 9 17:23:58 smpint-12 kernel: EXT3-fs (sdd1): error: ext3_journal_start_sb: Detected aborted journal Entity = demo_host | Entity Type = Host (Linux) | Log Source = Linux Syslog Logs | Host Name (Server) = smpint-12
Aug 9, 2017, 5:23:58 PM	Aug 9 17:23:58 smpint-12 kernel: EXT3-fs (sdd1): error: remounting filesystem read-only Entity = demo_host | Entity Type = Host (Linux) | Log Source = Linux Syslog Logs | Host Name (Server) = smpint-12

Page 2 of 2 (26-31 of 31 items) 1 2

You may have noticed that at 5:23:58PM, system logs (syslog) recorded that some I/O errors occurred on disk device sdd1 (see page 2), and database alert logs recorded that the database encountered I/O errors (see page 1); then at 5:24:00PM the database was terminated.

Where to Find Log Analytics Documentation

Log Analytics documentation including tutorials is available at the following URL:
https://docs.oracle.com/en/cloud/paas/management-cloud/log-analytics.html