

IBM Log Analysis with LogDNA

Cloud Native BootCamp

<https://cloudnative101.dev>

- **Legal Disclaimer © IBM Corporation 2020. All Rights Reserved.**
 - The information contained in this publication is provided for informational purposes only. While efforts were made to verify the completeness and accuracy of the information contained in this publication, it is provided AS IS without warranty of any kind, express or implied. In addition, this information is based on IBM's current product plans and strategy, which are subject to change by IBM without notice. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, this publication or any other materials. Nothing contained in this publication is intended to, nor shall have the effect of, creating any warranties or representations from IBM or its suppliers or licensors, or altering the terms and conditions of the applicable license agreement governing the use of IBM software.
 - References in this presentation to IBM products, programs, or services do not imply that they will be available in all countries in which IBM operates. Product release dates and/or capabilities referenced in this presentation may change at any time at IBM's sole discretion based on market opportunities or other factors, and are not intended to be a commitment to future product or feature availability in any way. Nothing contained in these materials is intended to, nor shall have the effect of, stating or implying that any activities undertaken by you will result in any specific sales, revenue growth or other results.

Applications generate huge amounts log data from the dynamic configurations and environments they run on. Availability is critical.

...and engineers need insights quickly

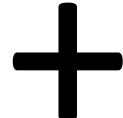
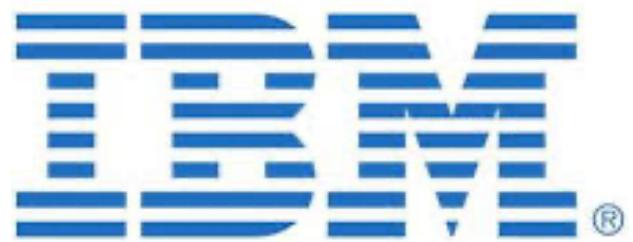
Data originates from complex environments

Huge amounts of data may take time to search for insights

Applications have very high availability objectives and to not perform slowly

Log data may be sensitive and subject to regulation and locality requirements

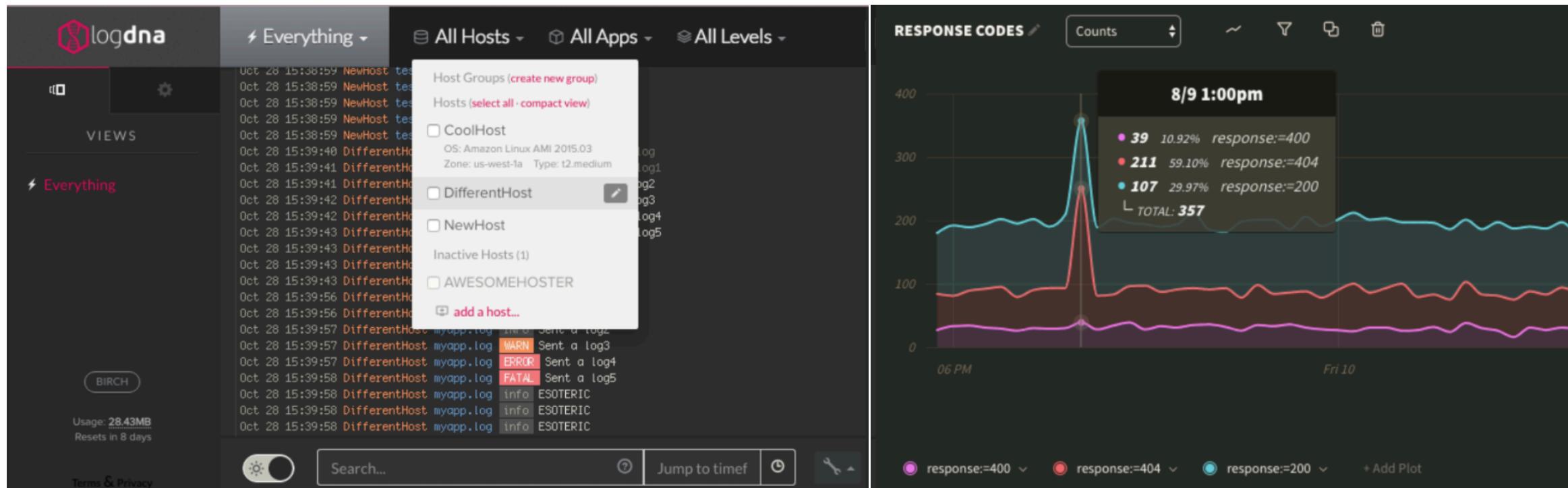
Partnership



IBM and LogDNA are delivering solutions to solve enterprise logging challenges to identify and fix issues faster

IBM Log Analysis with logDNA

Log management and analysis for debug of system and application issues



Optimized for modern Container based applications

Collect and aggregate data from any platform

Easily integrate with leading runtime environments

Expedite Insights with alerts and blazing fast search coupled with natural language query

Compliance, Archive, and Flexible Retention



LogDNA Highlights

Manage huge amounts of data from increasingly complex environments

Ingest log data from inside and outside IBM Cloud

- Application logs
 - Machine generated data
 - Containers, VMs, Bare Metal systems

Easily with:

- Automatic ingestion controls
 - Automatic parsing of common log formats
 - Automatic indexing of JSON objects

Optimized for Container based applications

Faster search than standard Elastic. Highly Scalable





LogDNA Highlights

Identify and pinpoint production issues more quickly

- **Alert into action** with multi-channel notification support through Pager Duty, Slack, webhooks and more
- Zoom in on activity events with Real-time **log tail** and filter functions
- Find and fix issues faster with **an intuitive query language** and lightning fast search.

Hosted to scale with your mission critical applications

- **Automated Archive** to IBM Cloud Storage
- **Flexible retention:** 7, 14, 30 days for log search
- **Pay per GB pricing**
- **Compliance:** GDPR, Privacy Shield, PCI, SOC2 Type 1

Pricing



PLAN	FEATURES	PRICING
30 day log retention	Logs are stored and searchable for 30 days Unlimited Hosts & Sources Live Streaming Tail Command Line (CLI) Tail Unlimited Saved Views Real Time Alerts	\$3.00 USD/Gigabyte-Month of logs ingested
14 day log retention	Logs are stored and searchable for 14 days Unlimited Hosts & Sources Live Streaming Tail Command Line (CLI) Tail Unlimited Saved Views Real Time Alerts	\$2.00 USD/Gigabyte-Month of logs ingested
7 day log retention	Logs are stored and searchable for 7 days Unlimited Hosts & Sources Live Streaming Tail Command Line (CLI) Tail Unlimited Saved Views Real Time Alerts	\$1.50 USD/Gigabyte-Month of logs ingested
Lite	Logs are not searchable, stored for 0 days, Unlimited Hosts & Sources, Live Streaming Tail, Command Line (CLI) Tail, 3 Saved Views, No Data Volume Limit	Free

Metered per actual consumption
Avoid subscription lock-ins and overage charges
Ingestion filters for reducing noise ahead of metered ingestion

Service Availability

IBM Log Analysis with LogDNA is deploying to multi-zone regional datacenters

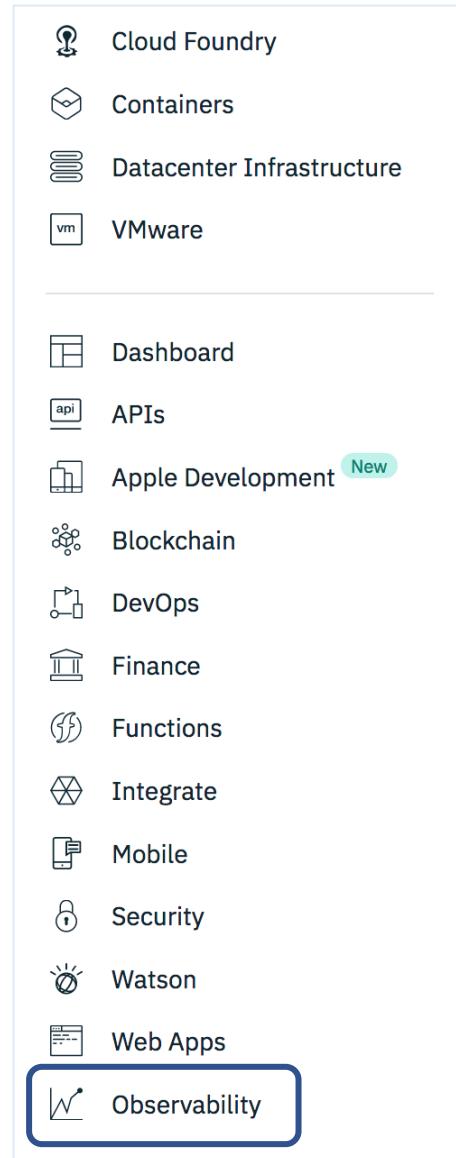
Available in NA-South today (Dallas)

Coming Soon:

- Germany (Frankfurt)
- United Kingdom (London)
- Asia Pacific North (Tokyo)
- Asia Pacific (Sydney)
- NA-East – (Washington DC)



Getting Started



IBM services with LogDNA are located in the Cloud Navigator in Observability

And find the offerings in the IBM Cloud catalog

A screenshot of the IBM Cloud catalog interface. On the left, there's a sidebar with 'All Categories (2) >' and a list of categories: Virtual Private Cloud, Compute, Containers, Networking, Storage, AI, Analytics, Databases, Developer Tools (1), Integration, Internet of Things, Security and Identity, Starter Kits, Web and Mobile, and Web and Application (1). The 'Developer Tools' category is expanded. On the right, there's a detailed view of the 'IBM Log Analysis with LogDNA' offering. It features the IBM logo, a hexagonal icon, the product name 'IBM Log Analysis with LogDNA', and a brief description: 'LogDNA provides log collection and log search for IBM Cloud Logging. Define alerts and design custom views to monitor application and ...'. A 'View Details' button is visible at the bottom of this card.

Topic Details

In presentation mode, click the tile for topic details. Click  menu to return here.

Prepare	Enable	Use
Instance Provision	Configure Log Sources	Alerting
Cluster Level Logging	Controlling what is Logged	Dashboarding
Managing Access	Ingest Logs by API	Live Log Tail
Launching Web UI	Migration from Legacy	Archiving & Exporting
Compliance		
Architecture & Data Management		

Start your journey today

- [IBM Log Analysis with LogDNA](#): Learn more
- [Observability in IBM Cloud](#): Explore LogDNA from within IBM Cloud
- [IBM Log Analysis with LogDNA in service catalog](#): Create a service instance
- [Documentation](#)

Thank you

Provisioning an instance

The screenshot displays the IBM Cloud interface with two main panels. On the left, the 'Catalog' panel shows a search bar for 'IBM Log Analysis' and a list of categories under 'Developer Tools'. A red box highlights the 'Developer Tools (1)' category. On the right, the 'Observability' panel shows an overview with tabs for 'Overview', 'Logging', and 'Monitoring'. A red box highlights the 'Observability' tab. Below the tabs, there is a detailed description of the 'IBM Log Analysis with LogDNA' service, which is a third-party tool for log collection and search. A red box highlights the 'Observability' section in the detailed description. At the bottom right of the 'Observability' panel, there is a 'Create logging instance' button.

IBM Cloud

Catalog Docs Support Manage

Catalog

IBM Log Analysis

All Categories (1) >

Developer Tools

IBM Log Analysis with LogDNA
Third Party

LogDNA provides log collection and log search for IBM Log Analysis. Define alerts and design custom views to monitor application and system logs.

Compute
Containers
Networking
Storage
AI
Analytics
Databases
Developer Tools (1)
Integration
Internet of Things
Security and Identity
Starter Kits
Web and Mobile
Web and Application

Dashboard
Resource List

Cloud Foundry
Kubernetes Cloud Foundry
Classic Infrastructure
VMware

APIs
Apple Development
Blockchain
DevOps
Finance
Functions
Integrate
Managed Solutions
Mobile

Observability

Logging
Monitoring

Observability

Get visibility into the performance and health of your resources. Troubleshoot apps and services, identify threats, detect performance issues, trigger alerts and more.

IBM Log Analysis with LogDNA

Use IBM Log Analysis with LogDNA to gain insights into your system and application logs.

Features include live logs, custom views, dashboards, and alerts. Choose from 7, 14, or 30 day log retention and have the ability to archive to IBM Cloud Object Storage to retain your logs for as long as you need. LogDNA integrates with IBM access control to quickly and tightly integrate into your application. [Learn more](#)

Create logging instance

NEW AREA

Provisioning an instance

The screenshot shows the IBM Cloud interface for provisioning a new instance of the "IBM Cloud Logging with LogDNA" service.

Header: IBM Cloud, Catalog, Docs, Support, Manage, Search for resource..., Randy Bertram's Account.

Title: IBM Cloud Logging with LogDNA
3rd Party - Standard

Details Section:

- Service name: myservice
- AUTHOR: LogDNA
- PUBLISHED DATE: 2/1/2018
- UPDATED DATE: 1/1/2017
- TYPE: Service
- Choose a region/location to deploy in: us-south
- Select a resource group: Default
- Feedback button

Locations Section:

- US South
- [View docs](#)
- [Terms and conditions](#)

Pricing Plans Section:

PLAN	FEATURES	PRICING
30 day log retention	Logs are stored and searchable for 30 days Unlimited Hosts & Sources Live Streaming Tail Command Line (CLI) Tail Unlimited Saved Views Real Time Alerts Archiving	\$3.00 USD/Gigabyte-Month of logs ingested

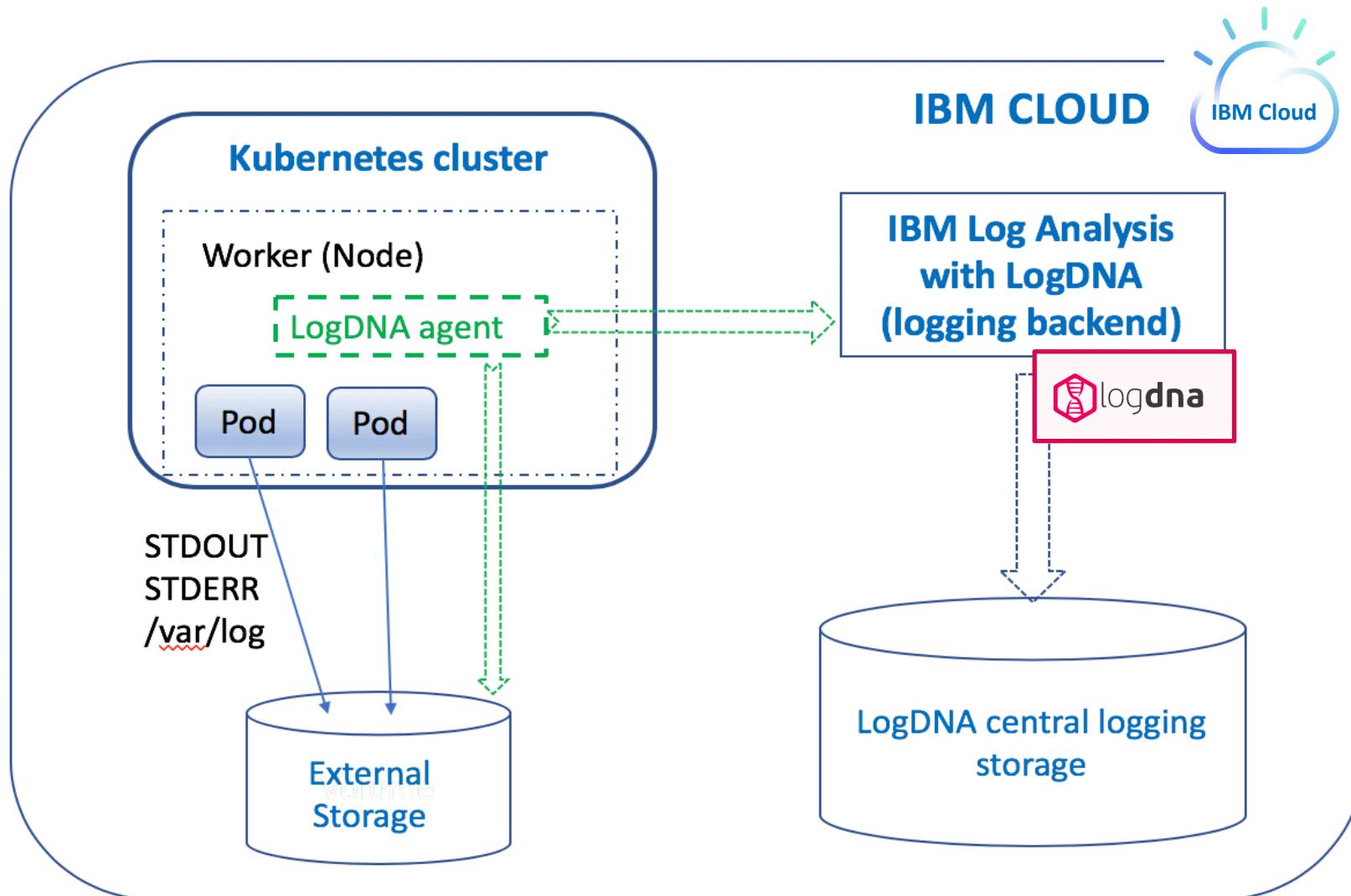
Bottom Navigation:

- Need help?
[Contact IBM Cloud Sales](#)
- [Estimate Monthly Cost](#)
[Cost Calculator](#)
- Create button

Provisioned instances

The screenshot shows the IBM Cloud Observability Logging interface. At the top, there's a navigation bar with links for Catalog, Docs, Support, and Manage, along with a search bar and a user account section for "Randy Bertram's Account". On the left, a sidebar menu is open, showing "Observability" and two sub-options: "Overview" and "Logging", with "Logging" currently selected. The main content area is titled "Logging" and includes a "LOCATION" dropdown set to "All Locations". On the right side of the main area, there are several buttons: "Create instance", "My Logs" (with a "View LogDNA" sub-link), "Edit log sources" (which is highlighted with a blue rectangular box), "View ingestion key", and "0 day log retention" (with a "Edit plan" link). A "FEEDBACK" button is located on the far right. At the bottom right, there's a yellow "Let's talk" button.

Cluster-level Logging for the IBM Cloud Kubernetes Service



Cluster-level Logging for the IBM Cloud Kubernetes Service

[menu](#)

IBM Cloud Catalog Docs Support Manage

Search for resource...

Randy Bertram's Account

LogDNA / My Logs - Edit sources

My Logs - Edit sources

Add agents to desired log sources

Logs from your desired log sources will feed into your logging instance: My Logs. Add LogDNA to your resources by following the individual instructions to install the LogDNA agents.

Linux Ubuntu/Debian	Kubernetes Ships logs from your Kubernetes v1.2+ cluster. This will automatically install a logdna-agent pod on each node of your cluster. <pre>kubectl create secret generic logdna-agent-key --from-literal=logdna-agent-key=daa8ad19fe51af620db8a84d49ab123a</pre> <pre>kubectl create -f https://raw.githubusercontent.com/logdna/logdna-agent/master/logdna-agent-ds.yaml</pre>
Linux RPM-based	
Linux Gentoo	
Kubernetes	
Docker	
Fluentd	
REST API	

For detailed information regarding the agent and configuration options, [check out our GitHub repo](#). Pro tip: You can configure [check out our GitHub repo](#) to tag your pods by adding LOGDNA_TAGS name and value (comma separated) under the env object.

FEEDBACK

Let's talk

Managing access from the IBM Cloud

IBM Cloud platform roles

Use the following table to identify the platform role that you can grant a user in the IBM Cloud to run any of the following platform actions:

Platform actions	IBM Cloud Platform Roles
Grant other account members access to work with the service	Administrator
Provision a service instance	Administrator Editor
Delete a service instance	Administrator Editor
Create a service ID	Administrator Editor
View details of a service instance	Administrator Editor Operator Viewer
View service instances in the Observability Logging dashboard	Administrator Editor Operator Viewer

IBM Cloud service roles

Use the following table to identify the service roles that you can grant a user to run any of the following service actions:

Actions	IBM Cloud Service Roles
Add LogDNA log sources	Manager
Archive logs	Manager
Renew the ingestion key	Manager
Configure alerts	Manager
Manage log data	Manager
Manage the LogDNA Web UI	Manager
View logs through the LogDNA Web UI	Manager Writer Reader

Launching the Web UI

menu

The screenshot shows the IBM Cloud Observability interface. At the top, there's a navigation bar with 'IBM Cloud' (with a dropdown), 'Catalog', 'Docs', 'Support', 'Manage', and a search bar 'Search for resource...'. On the left, a sidebar has 'Observability' selected under 'Logging'. The main area shows a 'Logging' section with a 'logdna-instance-01' entry, a 'View LogDNA' button, and a '2' indicating two log sources. Below this are buttons for 'Edit log sources', 'View ingestion key', and 'Edit plan'. A '7 day log rate' summary is also present. The bottom part of the interface shows a log viewer with a sidebar for navigating logs by source, tag, app, and level. A red box highlights the 'Observability' link in the sidebar.

IBM Cloud

Catalog Docs Support Manage

Search for resource...

☰ IBM Cloud

Observability

Overview

Logging

Monitoring

LOCATION All Locations

logdna-instance-01

View LogDNA

2

Edit log sources

View ingestion key

7 day log rate

Edit plan

☰

Find a View

Everything

All Tags

All Sources

All Apps

All Levels

DASHBOARD

EVERYTHING

VIEWS

KUBE VIEWS

VMS

UNCATEGORIZED

Observability

Security

Watson

Web Apps

Dashboard

Resource List

Cloud Foundry

Kubernetes

Classic Infrastructure

VMware

APIs

Apple Development

Blockchain

DevOps

Finance

Functions

Integrate

Managed Solutions

Mobile

menu

3

1

```
Nov 19 03:07:43 public-crf5e801f8870447328dc15bac335062f-alb1-7d7ccddc4c-9k2v1 nginx-ingress {"time_date": "2023-11-19T03:07:43Z", "source": "south.containers.appdomain.cloud", "level": "info", "log": "public-crf5e801f8870447328dc15bac335062f-alb1-7d7ccddc4c-9k2v1 nginx-ingress [0] time=2023-11-19T03:07:43Z level=info msg=\"[public-crf5e801f8870447328dc15bac335062f-alb1-7d7ccddc4c-9k2v1] received upstream status 0 from 54.032\""}\nNov 19 03:07:43 public-crf5e801f8870447328dc15bac335062f-alb1-7d7ccddc4c-9k2v1 nginx-ingress {"time_date": "2023-11-19T03:07:43Z", "source": "south.containers.appdomain.cloud", "level": "info", "log": "public-crf5e801f8870447328dc15bac335062f-alb1-7d7ccddc4c-9k2v1 nginx-ingress [0] time=2023-11-19T03:07:43Z level=info msg=\"[public-crf5e801f8870447328dc15bac335062f-alb1-7d7ccddc4c-9k2v1] received upstream status 0 from 54.032\""}\nNov 19 03:07:43 public-crf5e801f8870447328dc15bac335062f-alb1-7d7ccddc4c-9k2v1 nginx-ingress {"time_date": "2023-11-19T03:07:43Z", "source": "south.containers.appdomain.cloud", "level": "info", "log": "public-crf5e801f8870447328dc15bac335062f-alb1-7d7ccddc4c-9k2v1 nginx-ingress [0] time=2023-11-19T03:07:43Z level=info msg=\"[public-crf5e801f8870447328dc15bac335062f-alb1-7d7ccddc4c-9k2v1] received upstream status 0 from 54.032\""}\nNov 19 03:07:43 sysdig-agent-nwklh sysdig-agent 54.032, 1950, Information, sinsp_data_handler:60: ts=15421484\nNov 19 03:07:43 sysdig-agent-nwklh sysdig-agent 54.032, 1950, Information, sinsp_data_handler:64: Queue full,\nNov 19 03:07:43 calico-node-pb2rd calico-node INFO [53] int_dataplane.go 734: Applying dataplane updates
```

Configuring user preferences

Viewer Style

Viewer Options

Log Format

Default Contrast

Light Mode Dark Mode

Viewer Theme

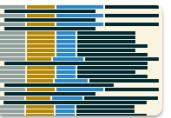
Customize the way your log viewer looks. Only you will see this.



Default



Monokai



Solarized

Viewer Style

Viewer Options

Log Format

Text Size

smaller  larger

Line Format

Configure the contents displayed for each line of the log viewer.

%time('MMM D HH:mm:ss') %source %app %level %line

Drag tokens below to rearrange line content ↴

%source %app %file %dyno %level %ip %iplocal

%time('YYYY-MM-DD HH:mm:ss')

%time('D/MM/YYYY:HH:mm:ss') %time('YYYY-MM-DD HH:mm:ss.SSS')

Viewer Style

Viewer Options

Log Format

Muted DEBUG statements

Checking this will show lines with log level of DEBUG in a lighter shade of color.

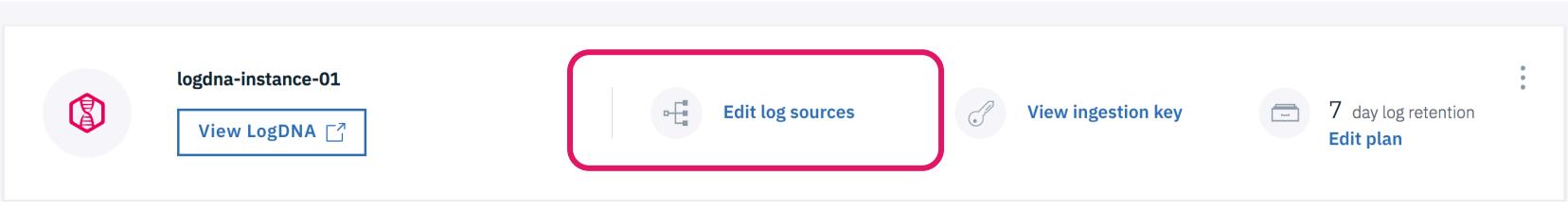
Show %time as UTC

Timestamps will be shown in UTC and timeframe searches will be done relative to UTC instead of local time.

Show raw line inside line context

Show the original line as it was received.

Configuring log sources to send logs



IBM Cloud Catalog Docs Support Manage Search for resource... Logging / logdna-instance-01 - Edit sources

logdna-instance-01 - Edit sources

Add agents to desired log sources

Logs from your desired log sources will feed into your logging instance: logdna-instance-01. Add LogDNA to your resources by following the individual instructions to install the LogDNA agents.

Platform	Description
Linux Ubuntu/Debian	
Linux RPM-based	
Kubernetes	Kubernetes Ships logs from your Kubernetes v1.2+ cluster. This will automatically install a logdna-agent pod on each node of your cluster. <pre>kubectl create secret generic logdna-agent-key --from-literal=logdna-agent-key=[object Object]</pre> <pre>kubectl create -f https://repo.logdna.com/ibm/prod/logdna-agent-ds-us-south.yaml</pre>

For detailed information regarding the agent and configuration options, [check out our GitHub repo](#). Pro tip: You can configure [our daemonset yaml](#) to tag your pods by adding a LOGDNA_TAGS name separated) under the env object.

Check LogDNA for updates once you successfully add or remove log sources. It may take a couple minutes.

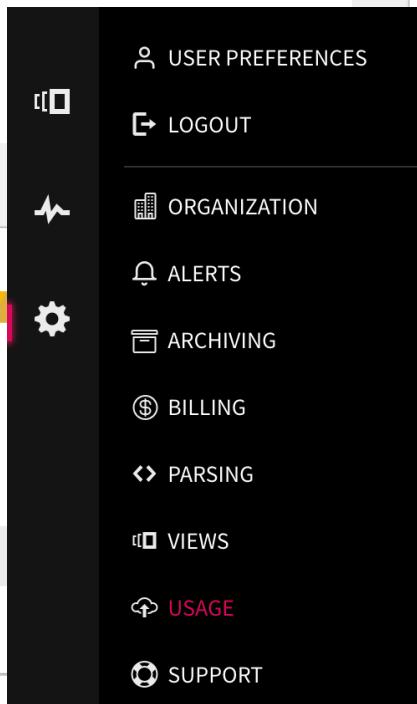
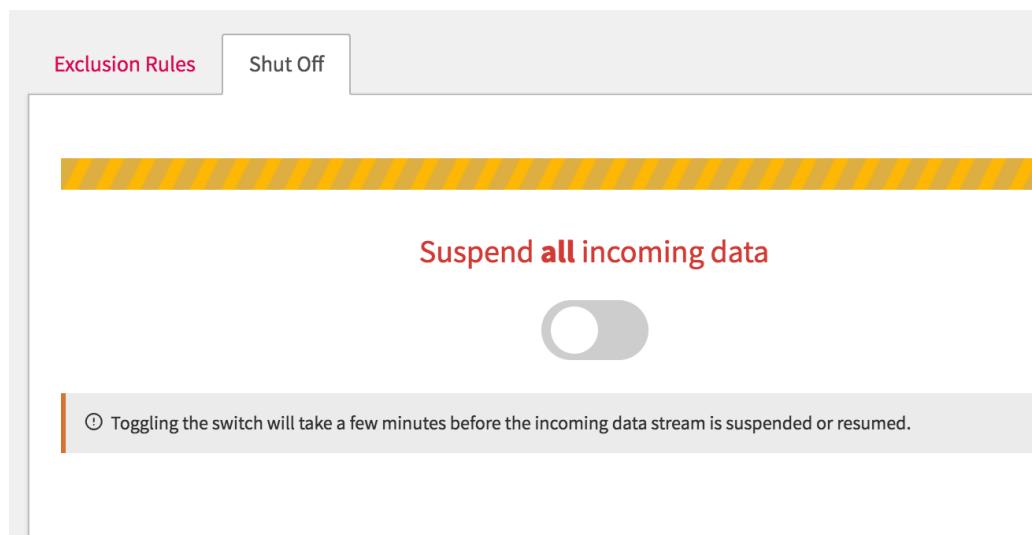
[View LogDNA](#) [Done](#)

Controlling what you log

Create exclusion rules.

- New lines that match an exclusion rule will not be stored and will not be archived.
- Excluded lines will not count toward your usage quota.
- New rules may take a few minutes to take effect.

Suspend all incoming data.



Sending log data by using the Ingestion API

```
curl "ENDPOINT/logs/ingest?QUERY_PARAMETERS" -u INGESTION_KEY: --header "Content-Type: application/json; charset=UTF-8" -d "LOG_LINES"
```

Region	Endpoint		
us-south	https://logs.us-south.logging.cloud.ibm.com		
Query parameter	Type	Status	Description
hostname	string	required	Host name of the source.
mac	string	optional	The network mac address of the host computer.
ip	string	optional	The local IP address of the host computer.
now	date-time	optional	The source unix timestamp in milliseconds at the time of the request. Used to calculate time drift.
tags	string	optional	Tags used to dynamically group hosts.
Query parameters			

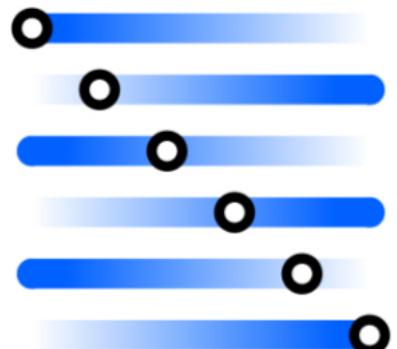
```
{
  "lines": [
    {
      "timestamp": "2018-11-02T10:53:06+00:00",
      "line": "This is my first log line.",
      "app": "myapp",
      "level": "INFO",
      "meta": {
        "customfield": { "nestedfield": "nestedvalue" }
      }
    }
  ]
}
```

```
curl "https://logs.us-south.logging.cloud.ibm.com/logs/ingest?hostname=MYHOST&now=$(date +%s)000" -u xxxxxxxxxxxxxxxxxxxxxxxx: --header "Content-Type: application/json; charset=UTF-8" -d "{\"lines\":[{\"line\":\"This is a sample test log statement\",\"timestamp\":\"2018-11-02T10:53:06+00:00\",\"level\":\"INFO\",\"app\":\"myapp\"}]}"
```

Migrating from the legacy service

menu

- You may run existing IBM Cloud Log Analysis parallel to IBM Log Analysis with LogDNA for duration of time it takes for real-time data to load LogDNA.
- You may download archived data and store in your own Cloud Object Storage account.
- IBM Cloud Log Analysis and LogDNA APIs are different so clients may need to make necessary adjustments to their implementation.



Alerts and notification Channels

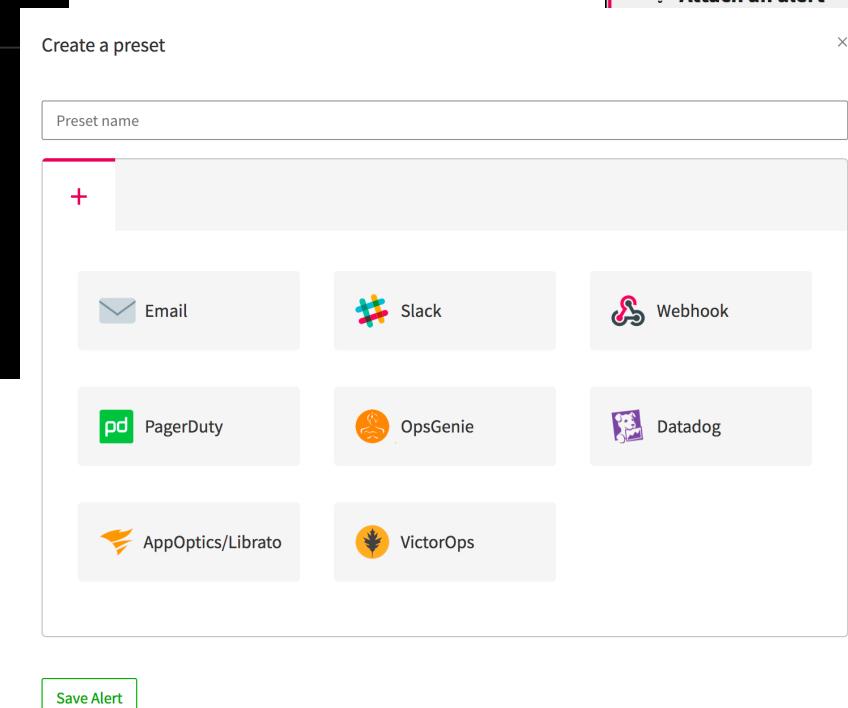
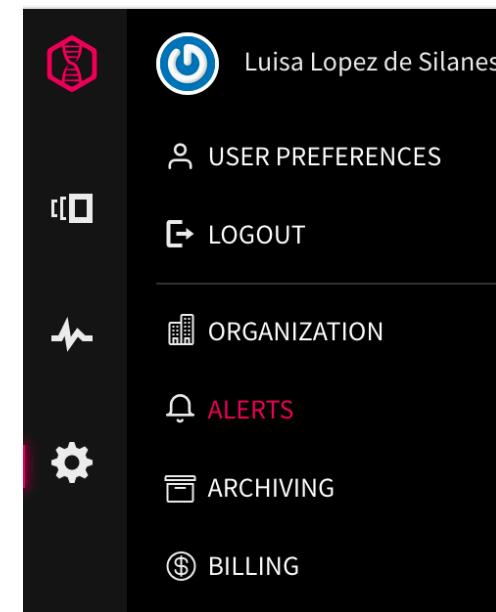
You can configure any of the following conditions for an alert:

- ***Time frequency***: Specify how often to trigger an alert.

Valid values are: 30 seconds, 1 minute, 5 minutes, 15 minutes, 30 minutes, 1 hour, 6 hours, 12 hours, 24 hours

- ***Log lines counter***: Specify the number of log lines that match the view's filtering and search criteria.

When the number of log lines is reached, an alert is triggered.



You can decide whether both conditions are checked or only one. If both conditions are set, an alert is triggered when any of the thresholds is reached.

Graphing and Dashboards

Create graphs with ease.

Directly use your same search queries to generate graphs

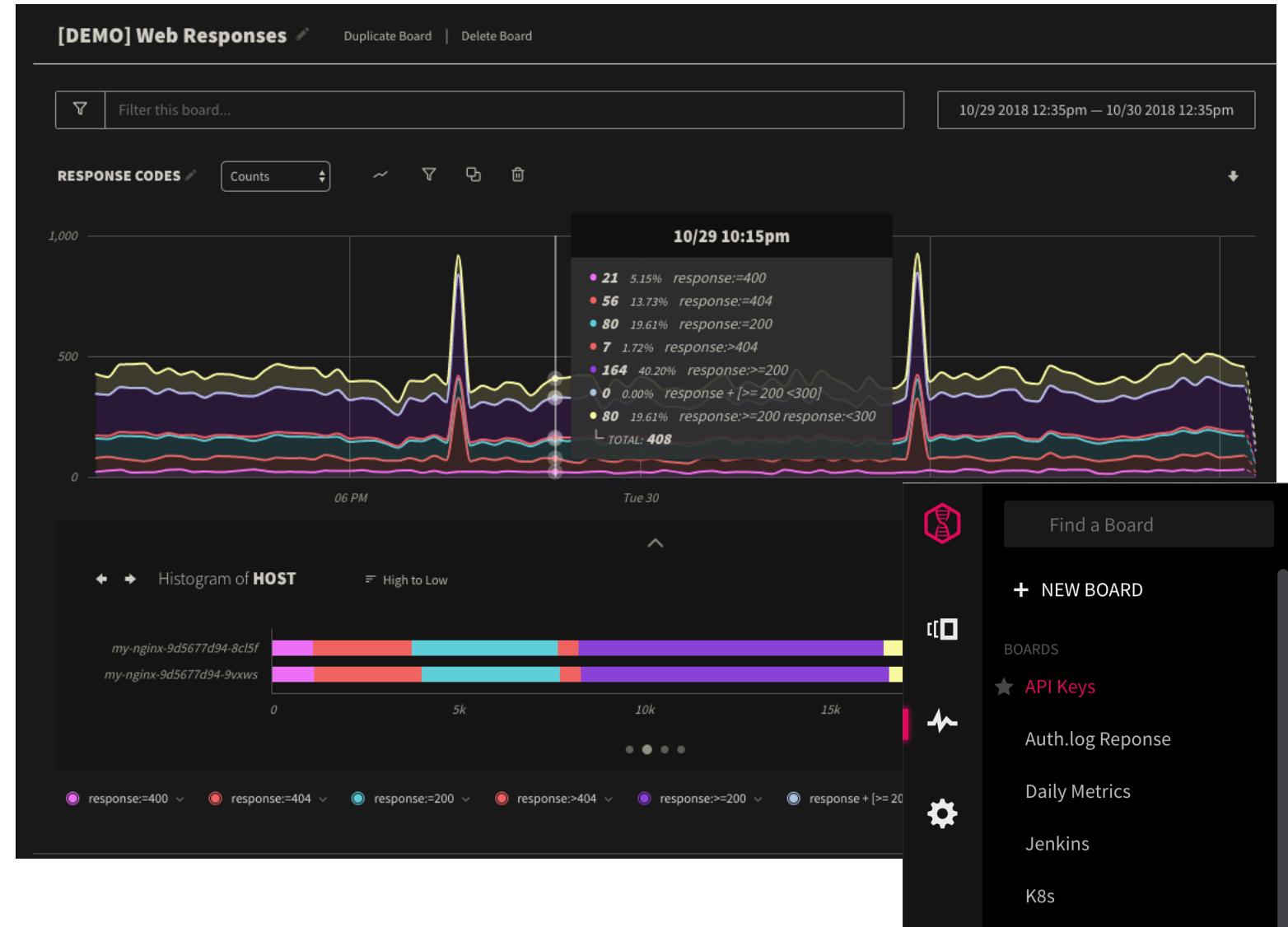
Stack additional graphs and queries to perform direct comparisons in a scoped window

Save multiple graphs into a single board

Advanced analysis capabilities

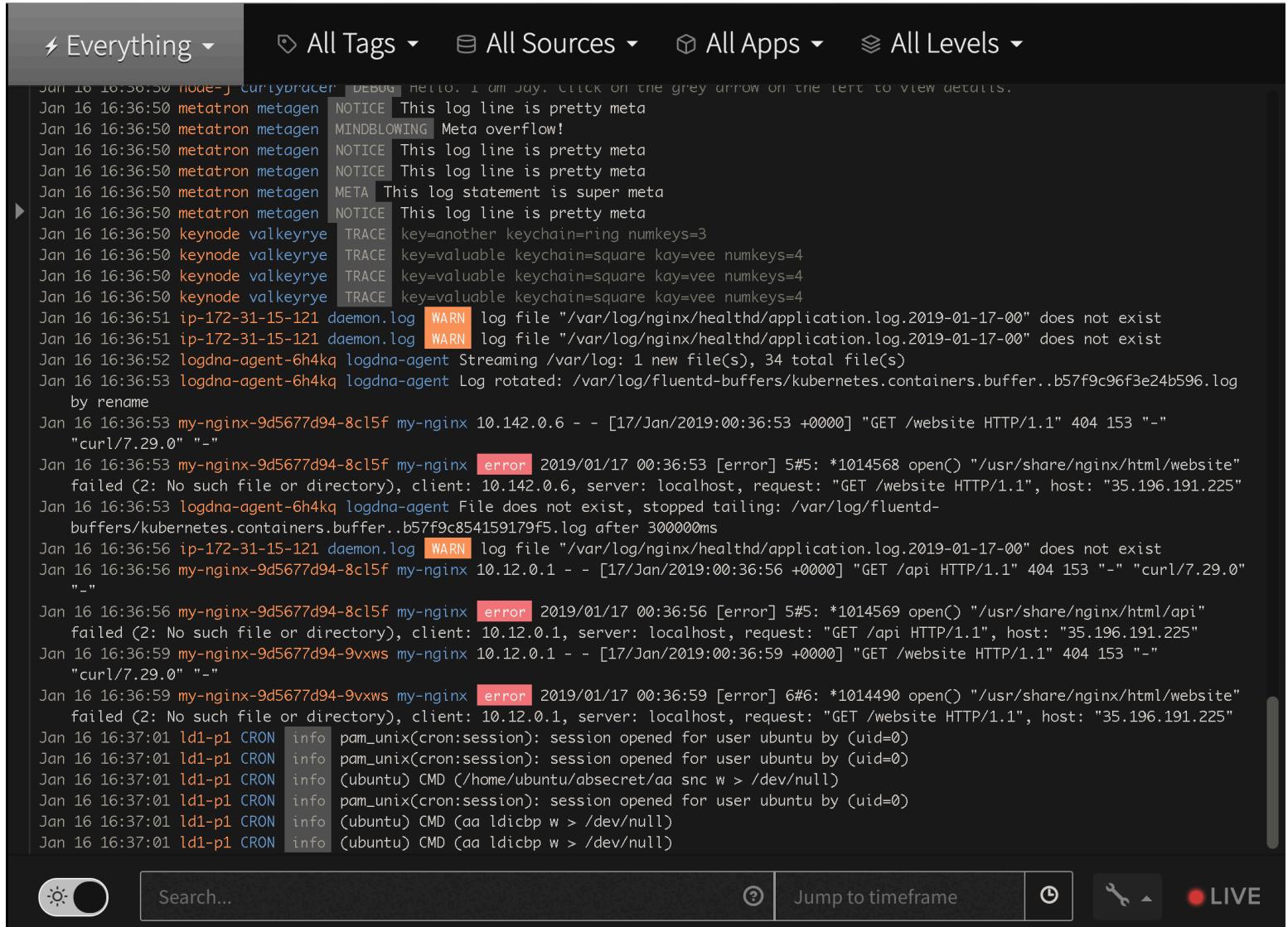
Create histograms against auto parsed fields to compare another variable

Filter and exclude parameters across a set graphs within a board



Live Log Tail

- Stream all your logs in real-time
- Use live tail to check on application and system health by watching a replay of your logs
- Average live tail latency of ~1s, Logs are parsed and streamed back out to the users while log data is being indexed for search in the backend
- Seamlessly scroll back and forward between previous and live logs



The screenshot shows a log tailing interface with the following features and data:

- Filtering:** Top navigation bar includes dropdowns for "Everything", "All Tags", "All Sources", "All Apps", and "All Levels".
- Log Data:** The main area displays log entries from January 16, 2019, at 16:36:50. The logs are color-coded by type (e.g., DEBUG, NOTICE, WARNING, ERROR) and source (e.g., curlpracer, metatron, logdagent, my-nginx).
- Annotations:** A note in the top right says: "Click on the grey arrow on the left to view details."
- Search:** Bottom left has a search bar with placeholder "Search...".
- Timeframe:** Bottom center has a "Jump to timeframe" button with a question mark icon.
- Tools:** Bottom right includes icons for a wrench (Edit), a circular arrow (Refresh), and a red dot with "LIVE" text.

```

Jan 16 16:36:50 node-j curlpracer DEBUG hello, I am Jay. Click on the grey arrow on the left to view details.
Jan 16 16:36:50 metatron metagen NOTICE This log line is pretty meta
Jan 16 16:36:50 metatron metagen MINDBLOWING Meta overflow!
Jan 16 16:36:50 metatron metagen NOTICE This log line is pretty meta
Jan 16 16:36:50 metatron metagen NOTICE This log line is pretty meta
Jan 16 16:36:50 metatron metagen META This log statement is super meta
Jan 16 16:36:50 metatron metagen NOTICE This log line is pretty meta
Jan 16 16:36:50 keynode valkeyrye TRACE key=another keychain=ring numkeys=3
Jan 16 16:36:50 keynode valkeyrye TRACE key=valuable keychain=square key=vee numkeys=4
Jan 16 16:36:50 keynode valkeyrye TRACE key=valuable keychain=square key=vee numkeys=4
Jan 16 16:36:50 keynode valkeyrye TRACE key=valuable keychain=square key=vee numkeys=4
Jan 16 16:36:51 ip-172-31-15-121 daemon.log WARN log file "/var/log/nginx/healthd/application.log.2019-01-17-00" does not exist
Jan 16 16:36:51 ip-172-31-15-121 daemon.log WARN log file "/var/log/nginx/healthd/application.log.2019-01-17-00" does not exist
Jan 16 16:36:52 logdagent-6h4kq logdagent Streaming /var/log: 1 new file(s), 34 total file(s)
Jan 16 16:36:53 logdagent-6h4kq logdagent Log rotated: /var/log/fluentd-buffers/kubernetes.containers.buffer..b57f9c96f3e24b596.log by rename
Jan 16 16:36:53 my-nginx-9d5677d94-8cl5f my-nginx 10.142.0.6 - - [17/Jan/2019:00:36:53 +0000] "GET /website HTTP/1.1" 404 153 "-" "curl/7.29.0" "-"
Jan 16 16:36:53 my-nginx-9d5677d94-8cl5f my-nginx error 2019/01/17 00:36:53 [error] 5#5: *1014568 open() "/usr/share/nginx/html/website" failed (2: No such file or directory), client: 10.142.0.6, server: localhost, request: "GET /website HTTP/1.1", host: "35.196.191.225"
Jan 16 16:36:53 logdagent-6h4kq logdagent File does not exist, stopped tailing: /var/log/fluentd-buffers/kubernetes.containers.buffer..b57f9c854159179f5.log after 300000ms
Jan 16 16:36:56 ip-172-31-15-121 daemon.log WARN log file "/var/log/nginx/healthd/application.log.2019-01-17-00" does not exist
Jan 16 16:36:56 my-nginx-9d5677d94-8cl5f my-nginx 10.12.0.1 - - [17/Jan/2019:00:36:56 +0000] "GET /api HTTP/1.1" 404 153 "-" "curl/7.29.0" "-"
Jan 16 16:36:56 my-nginx-9d5677d94-8cl5f my-nginx error 2019/01/17 00:36:56 [error] 5#5: *1014569 open() "/usr/share/nginx/html/api" failed (2: No such file or directory), client: 10.12.0.1, server: localhost, request: "GET /api HTTP/1.1", host: "35.196.191.225"
Jan 16 16:36:59 my-nginx-9d5677d94-9vxws my-nginx 10.12.0.1 - - [17/Jan/2019:00:36:59 +0000] "GET /website HTTP/1.1" 404 153 "-" "curl/7.29.0" "-"
Jan 16 16:36:59 my-nginx-9d5677d94-9vxws my-nginx error 2019/01/17 00:36:59 [error] 6#6: *1014490 open() "/usr/share/nginx/html/website" failed (2: No such file or directory), client: 10.12.0.1, server: localhost, request: "GET /website HTTP/1.1", host: "35.196.191.225"
Jan 16 16:37:01 ld1-p1 CRON info pam_unix(cron:session): session opened for user ubuntu by (uid=0)
Jan 16 16:37:01 ld1-p1 CRON info pam_unix(cron:session): session opened for user ubuntu by (uid=0)
Jan 16 16:37:01 ld1-p1 CRON info (Ubuntu) CMD (/home/ubuntu/absecret/aa snc w > /dev/null)
Jan 16 16:37:01 ld1-p1 CRON info pam_unix(cron:session): session opened for user ubuntu by (uid=0)
Jan 16 16:37:01 ld1-p1 CRON info (Ubuntu) CMD (aa ldicbp w > /dev/null)
Jan 16 16:37:01 ld1-p1 CRON info (Ubuntu) CMD (aa ldicbp w > /dev/null)

```

Archiving data

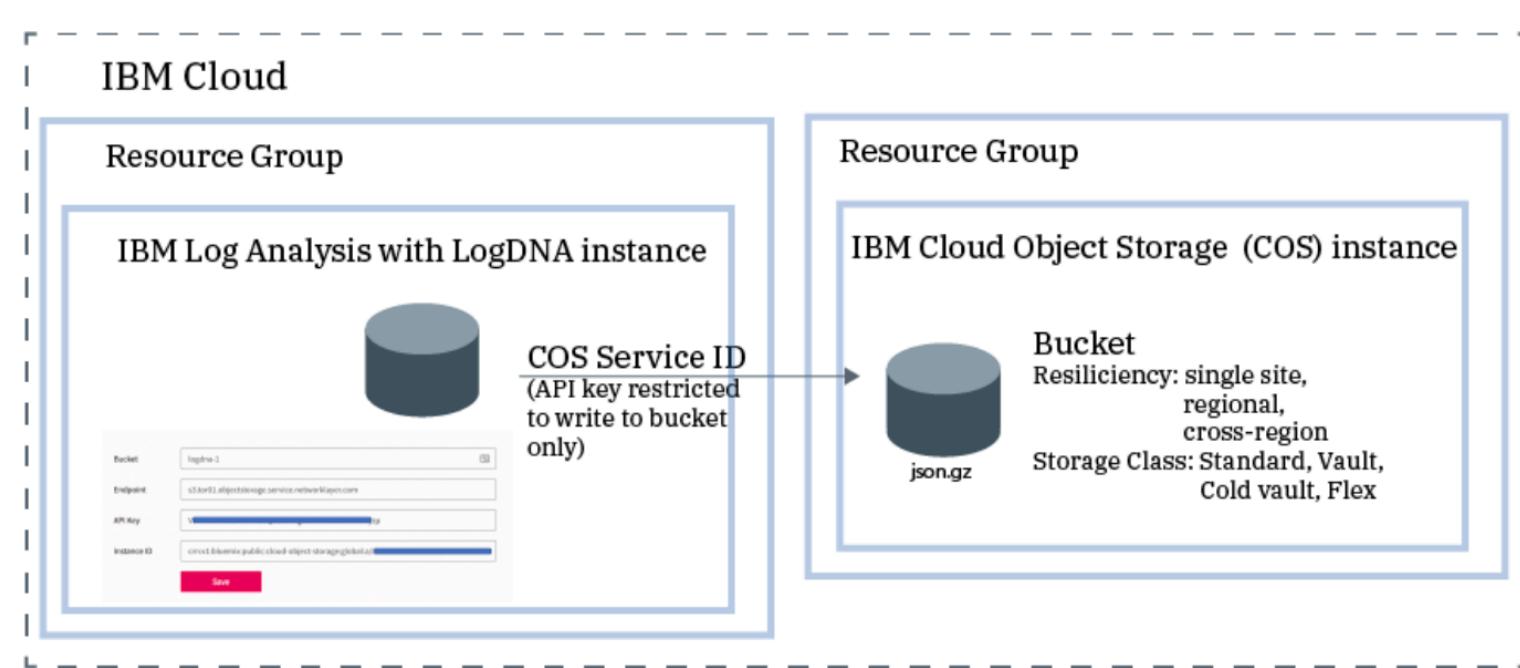
⚠ Archiving automatically exports your logs each night. Once configured, your exported logs will appear within 24-48 hours. Check out our [archiving guide](#) for more info.

IBM Cloud Object Storage

- In the [IBM Cloud Catalog](#), provision an instance (or use an existing one) of the [IBM Cloud Storage \(COS\)](#) service
- From the [IBM Cloud Dashboard](#), select the COS instance and create a new bucket. Enter the bucket name in the *Bucket* field
- While inside the COS Dashboard, select the bucket and then view the bucket configuration. Copy any private endpoint to the *Endpoint* field
- From the COS UI, go to the Service Credentials tab, and create a new service ID. Then, restrict that service ID to Write on the bucket. After the serviceID is created, view the serviceID details and copy the apikey value to the *API Key* field, and the resource_instance_id to the *Instance ID* field

Bucket (i.e. my-archiving-bucket)
Endpoint (i.e. s3-api.us-geo.objectstorage.softlayer.net)
API Key API Key
Instance ID Resource Instance ID
Save

You can archive logs from an IBM Log Analysis with LogDNA instance into a bucket in an IBM Cloud Object Storage (COS) instance.



To configure archiving, you must have an IAM policy with platform role **Viewer** and service role **Manager** for the IBM Log Analysis with LogDNA service.

Each IBM Log Analysis with LogDNA instance has its own archiving configuration.

Logs are automatically archived once a day in a compressed format (**.json.gz**). Each line preserves its metadata.

Logs are archived within 24-48 hours after you save the configuration.

Reading archived logs

Log files are stored in a zipped JSON lines format.

<input type="checkbox"/>	Object Name	Size	Last Modified	
<input type="checkbox"/>	4cfade7f77.2018-10-23.60.json.gz	29.2 MB	10/24/2018 1:37:13 AM	...
<input type="checkbox"/>	4cfade7f77.2018-10-24.60.json.gz	92.0 MB	10/25/2018 1:39:19 AM	Details
<input type="checkbox"/>	4cfade7f77.2018-10-25.60.json.gz	88.4 MB	10/26/2018 1:39:16 AM	SQL URL
<input type="checkbox"/>	4cfade7f77.2018-10-26.60.json.gz	73.1 MB	10/27/2018 1:38:44 AM	Download

To view log entries that are archived:

1. Download an archived file
2. Uncompressed the file
3. Use a tool that parses JSON.

Some tools that you can use to read log entries:

- **jq** (command line tool)
- **Visual Studio Code**

Exporting log data

You can **export** a set of log entries **from the web UI** or **programmatically**.

To define the set of data that you want to export, you can apply filters and searches, and specify the time range.

When you **export logs from the Web UI**, you get an email that is sent to your email address, with a link to a compressed file that includes the data. To get the data, you must click the link and download the compressed file.

When you **export logs programmatically**, you can choose to send an email or to stream logs into your terminal.

The compressed log file containing the data that you want to export is available for a maximum of 48 hours.

The maximum number of lines that you can export is 10,000.

Export Lines

Sources: MYHOST

Time Range for Export

11/15 2018 5:56pm – 11/16 2018 5:56pm

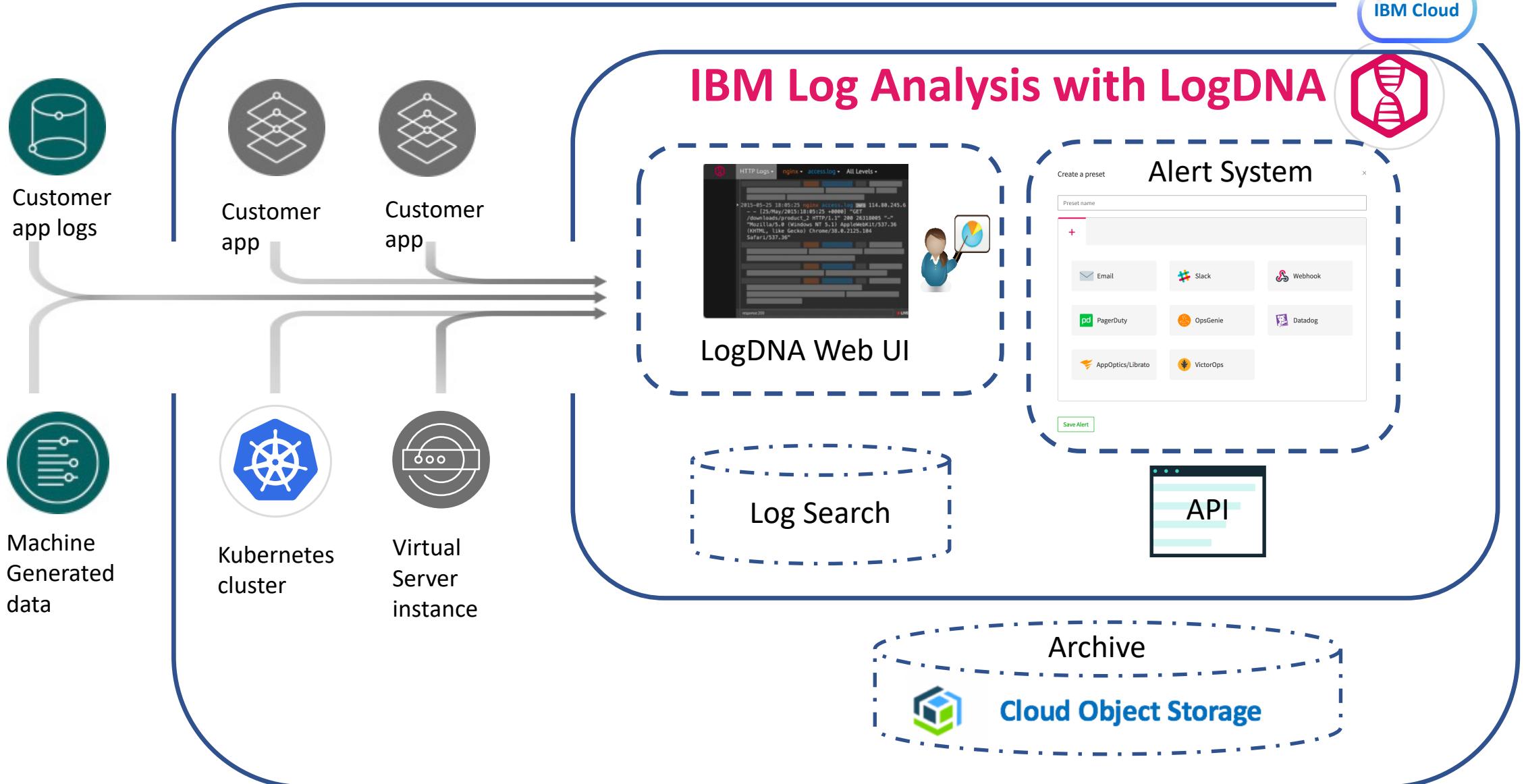
Prefer newer lines

* If your export exceeds the 10,000 line limit

Exported lines will be emailed to **lopezdsr@uk.ibm.com** once completed as a compressed **.jsonl** file.

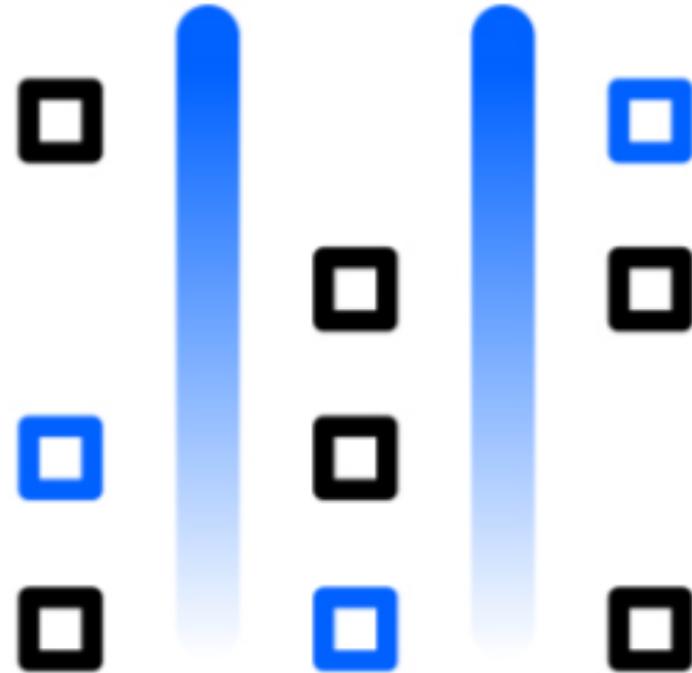
Request Export

Log data may be collected from inside and outside IBM Cloud



Data Management

- Data in motion and data at rest are encrypted, in compliance with IBM Cloud security standards.
- API tools for retention management.
- Data co-residency with cloud workloads.
- Control access to data by integrating with IBM Cloud IAM.
- Archiving log data to customer owned Object Storage buckets, can be configured with BYOK



Compliance



Security Standards
Council



Use the IBM Log Analysis with LogDNA service to add enhanced logging capabilities to the IBM Cloud

- ✓ Collect and aggregate logs in a centralized system.
- ✓ Troubleshoot logs in real-time to diagnose issues and identify problems.
- ✓ Issue alerts to be notified of important actions.
- ✓ Export logs to a local file for analysis or to an archive service to meet compliance and auditing requirements.
- ✓ Control logging infrastructure costs by customizing what logs to manage through IBM Log Analysis with LogDNA.

Find a View

⚡ Everything ▾

⌚ All Tags ▾

☷ All Sources ▾

⬢ All Apps ▾

≣ All Levels ▾

DASHBOARD

EVERYTHING

VIEWS

▶ DEMO

▶ SECURITY

e468f585-7acd-4e6c-b458-... TRIAL (7 days left)

Oct 1 18:24:03 calico-node-f7wxt calico-node [INFO] ipsets.go:90: Finished resync family=inet numInconsistenciesFound=0 resyncDuration=2.296522ms

Oct 1 18:24:03 calico-node-hwfrx calico-node [INFO] [50] int_dataplane.go:748: Finished applying updates to dataplane. msecToApply=2.898796

Oct 1 18:24:04 kubernetes-dashboard-74847f67d6-g76vn kubernetes-dashboard 2018/10/01 22:24:04 Restarting synchronizer: kubernetes-dashboard-key-holder-kube-system.

Oct 1 18:24:04 kubernetes-dashboard-74847f67d6-g76vn kubernetes-dashboard 2018/10/01 22:24:04 Starting secret synchronizer for kubernetes-dashboard-key-holder in namespace kube-system

Oct 1 18:24:04 kubernetes-dashboard-74847f67d6-g76vn kubernetes-dashboard 2018/10/01 22:24:04 Synchronizer kubernetes-dashboard-key-holder-kube-system exited with error: kubernetes-dashboard-key-holder-kube-system watch ended with timeout

Oct 1 18:24:06 kube-dal10-crb3d749537ccb4092af5b2b8002ab098d-w2 kubelet.log I1001 22:24:05.057785 1600 server.go:796] GET /stats/summary/: (17.703138ms) 200 [[Go-http-client/1.1] 10.94.14.2:49710]

Oct 1 18:24:06 kube-dal10-crb3d749537ccb4092af5b2b8002ab098d-w2 syslog I1001 22:24:05.057785 1600 server.go:796] GET /stats/summary/: (17.703138ms) 200 [[Go-http-client/1.1] 10.94.14.2:49710]

Oct 1 18:24:08 kubernetes-dashboard-74847f67d6-g76vn kubernetes-dashboard 2018/10/01 22:24:08 Restarting synchronizer: kubernetes-dashboard-key-holder-kube-system.

Oct 1 18:24:08 kubernetes-dashboard-74847f67d6-g76vn kubernetes-dashboard 2018/10/01 22:24:08 Starting secret synchronizer for kubernetes-dashboard-key-holder in namespace kube-system

Oct 1 18:24:08 kubernetes-dashboard-74847f67d6-g76vn kubernetes-dashboard 2018/10/01 22:24:08 Synchronizer kubernetes-dashboard-key-holder-kube-system exited with error: kubernetes-dashboard-key-holder-kube-system watch ended with timeout

Oct 1 18:24:06 calico-node-4pf6t calico-node [INFO] [49] int_dataplane.go:734: Applying dataplane updates

Oct 1 18:24:06 calico-node-4pf6t calico-node [INFO] [49] ipsets.go:223: Asked to resync with the dataplane on next update. family="inet"

Oct 1 18:24:06 calico-node-4pf6t calico-node [INFO] [49] ipsets.go:254: Resyncing ipsets with dataplane. family="inet"

Oct 1 18:24:06 calico-node-4pf6t calico-node [INFO] [49] ipsets.go:304: Finished resync family="inet" numInconsistenciesFound=0 resyncDuration=1.107139ms

Oct 1 18:24:06 calico-node-4pf6t calico-node [INFO] [49] int_dataplane.go:748: Finished applying updates to dataplane. msecToApply=2.060631

Oct 1 18:24:06 kubernetes-dashboard-74847f67d6-g76vn kubernetes-dashboard 2018/10/01 22:24:06 Restarting synchronizer: kubernetes-dashboard-key-holder-kube-system.

Oct 1 18:24:06 kubernetes-dashboard-74847f67d6-g76vn kubernetes-dashboard 2018/10/01 22:24:06 Starting secret synchronizer for kubernetes-dashboard-key-holder in namespace kube-system

Oct 1 18:24:06 kubernetes-dashboard-74847f67d6-g76vn kubernetes-dashboard 2018/10/01 22:24:06 Synchronizer kubernetes-dashboard-key-holder-kube-system exited with error: kubernetes-dashboard-key-holder-kube-system watch ended with timeout

Oct 1 18:24:11 calico-node-hwfrx calico-node [INFO] [50] health.go:150: Overall health summary=&health.HealthReport{Live:true, Ready:true}

Search... ⌚

⌚ Jump to timeframe... ⌚

🔧 🔧

LIVE ● LIVE

Find a View

⚡ Everything ▾

🕒 All Tags ▾

☷ All Sources ▾

⬢ All Apps ▾

≣ All Levels ▾

DASHBOARD

EVERYTHING

VIEW

▶ DEMO

▶ SECURITY

Oct 1 18:24:35 calico-node-hwfr calico-node [INFO] [50] ipsets.go 254: Resyncing ipsets with dataplane. family="inet"
Oct 1 18:24:35 calico-node-hwfr calico-node [INFO] [50] ipsets.go 304: Finished resync family="inet" numInconsistenciesFound=0
resyncDuration=2.628497ms
Oct 1 18:24:35 calico-node-hwfr calico-node [INFO] [50] int_dataplane.go 748: Finished applying updates to dataplane.
msecToApply=3.0222759999999997

View in context Copy to clipboard Share this line Close

msecToApply 3.0222759999999997

LINE IDENTIFIERS

Source calico-node-hwfr App calico-node

File /var/log/containers/calico-n + - calico-node-340f4fd998ba007b452d4893fcec26080bc4fc3b38b69272da52c8e4f4c0c7f.log

Pod calico-node-hwfr Container calico-node Namespace kube-system Node kube-dal10-crb3d749537ccb4092af5b2b8002ab098d-w3

Container ID 340f4fd998b

TAGS

k8s

LABELS

JSON

image c6abe3f286354f464ba01a92e1a417721de5f13c1db21a1cb7cb37a8fb1f2e33 k8s-app calico-node

Oct 1 18:24:38 calico-node-hwfr calico-node [INFO] [50] health.go 150: Overall health summary=&health.HealthReport{Live:true, Ready:true}
Oct 1 18:24:42 kubernetes-dashboard-74847f67d6-g76vn kubernetes-dashboard 2018/10/01 22:24:42 Restarting synchronizer: kubernetes-dashboard-key-holder-kube-system.
Oct 1 18:24:42 kubernetes-dashboard-74847f67d6-g76vn kubernetes-dashboard 2018/10/01 22:24:42 Starting secret synchronizer for kubernetes-dashboard-key-holder in namespace kube-system
Oct 1 18:24:42 kubernetes-dashboard-74847f67d6-g76vn kubernetes-dashboard 2018/10/01 22:24:42 Synchronizer kubernetes-dashboard-key-holder kube-system exited with error. Kubernetes dashboard key holder kube-system watch ended with timeout

⚠ e468f585-7acd-4e6c-b458-... TRIAL (7 days left)

Search...

⌚ Jump to timeframe...

🔧

● LIVE

