IBM Log Analysis with  LogDNA

Cloud Native BootCamp

https://cloudnative101.dev

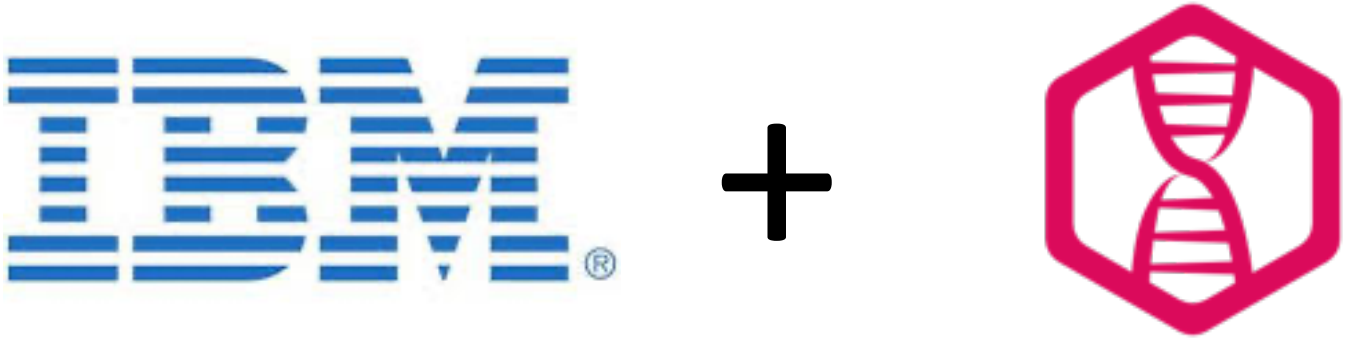
- **Legal Disclaimer © IBM Corporation 2020. All Rights Reserved.**
  - The information contained in this publication is provided for informational purposes only. While efforts were made to verify the completeness and accuracy of the information contained in this publication, it is provided AS IS without 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

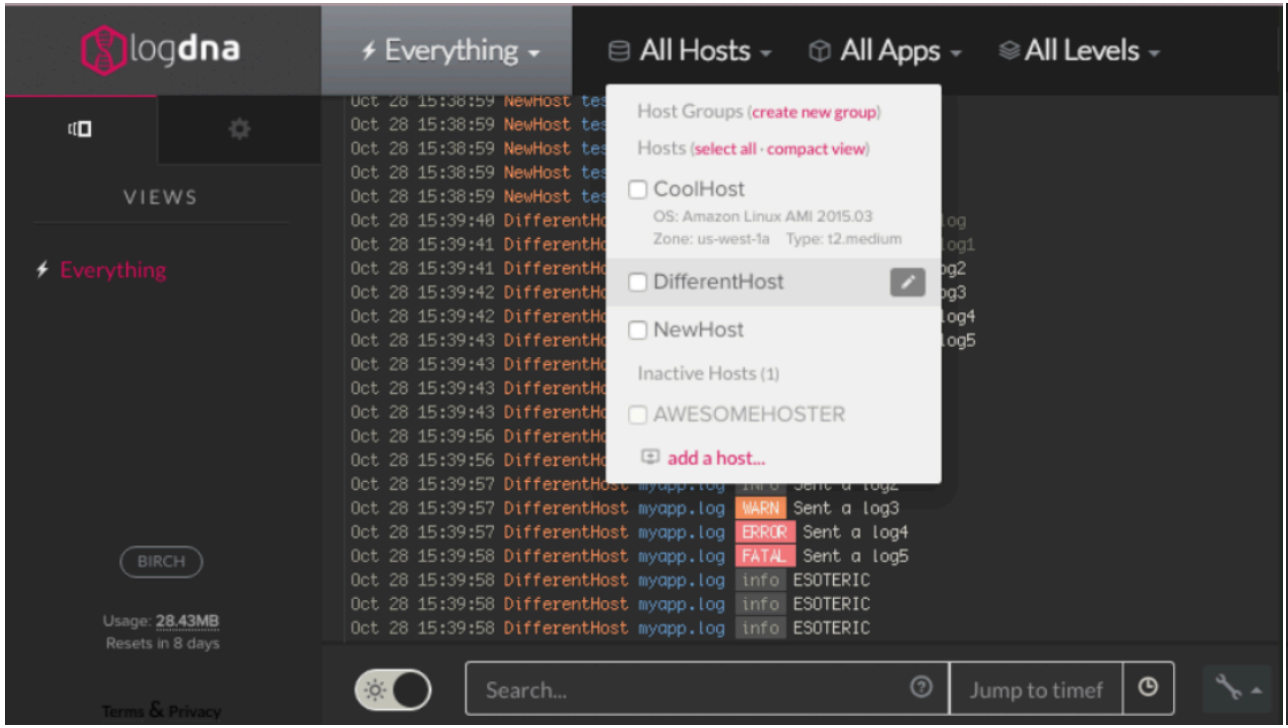
Partnership

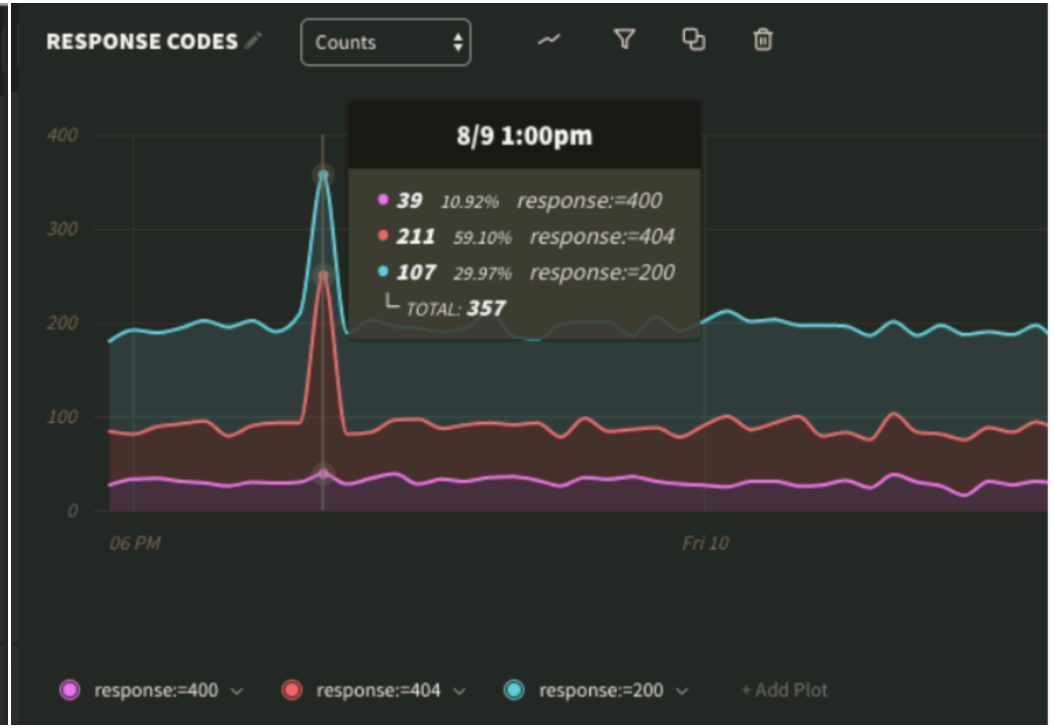


IBM and LogDNA are delivering solutions to solve enterprise logging challenges to identify and fix issues faster

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 Streaminig 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

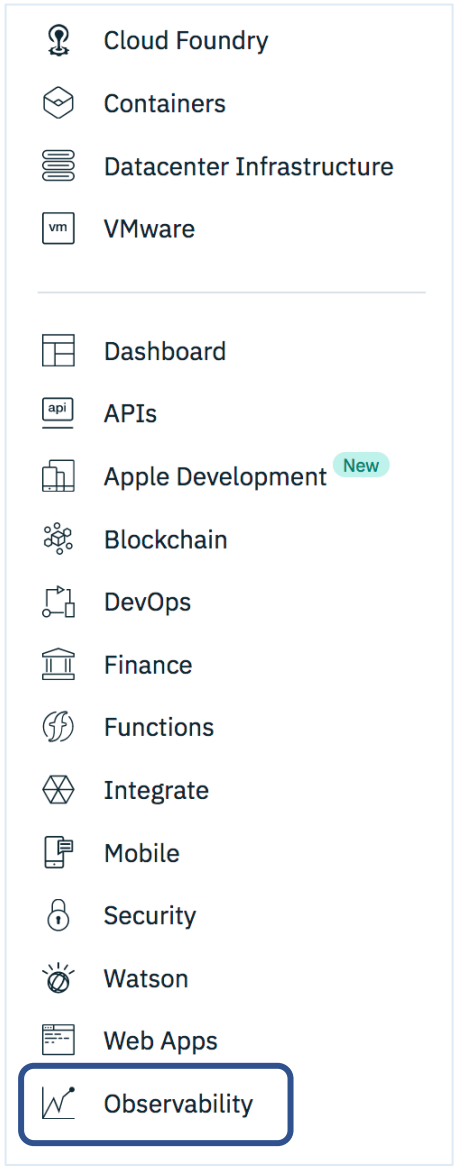
IBM Log Analysis with LogDNA is deploying to multi-zone regional datacenters

Available in NA-South today (Dallas)

Coming Soon:

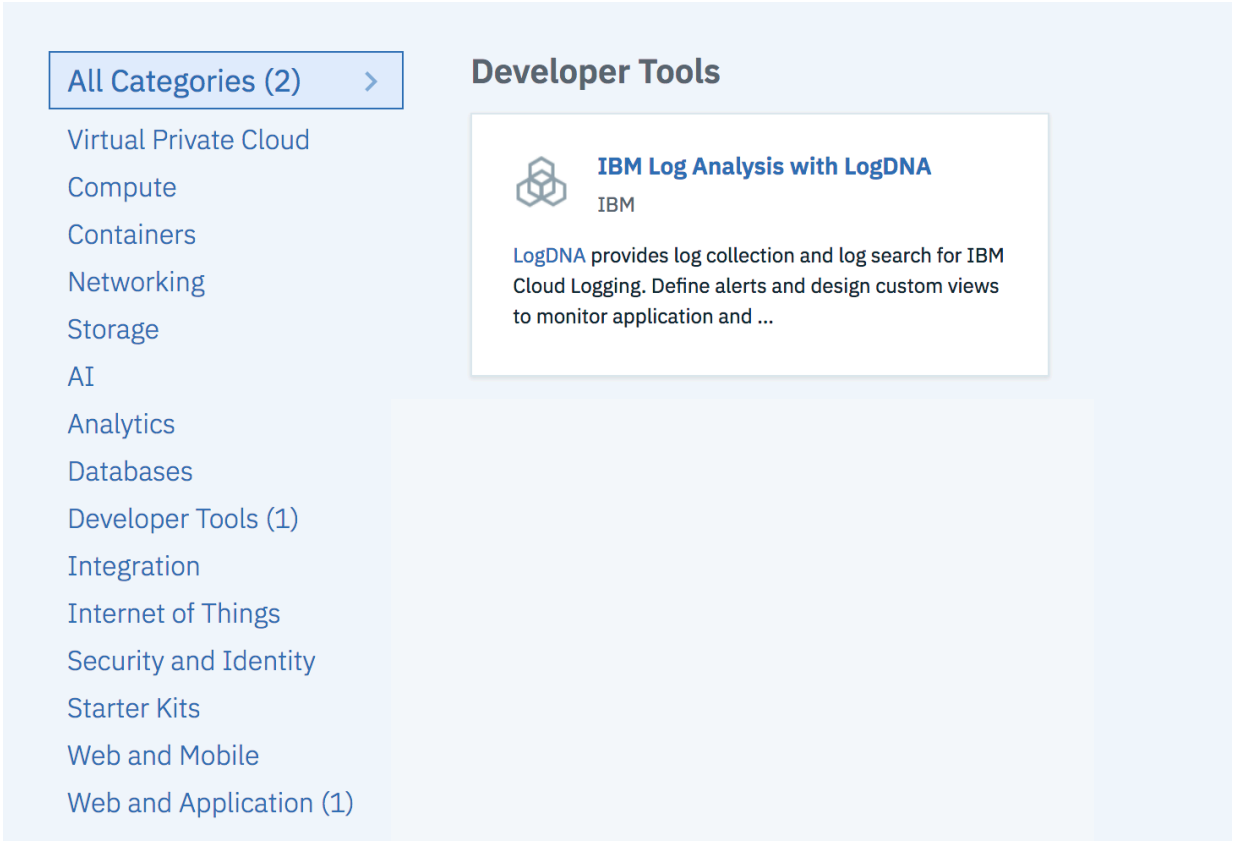
- Germany (Frankfurt)
- United Kingdom (London)
- Asia Pacific North (Toyko)
- Asia Pacific (Sydney)
- NA-East – (Washington DC)

Getting Started



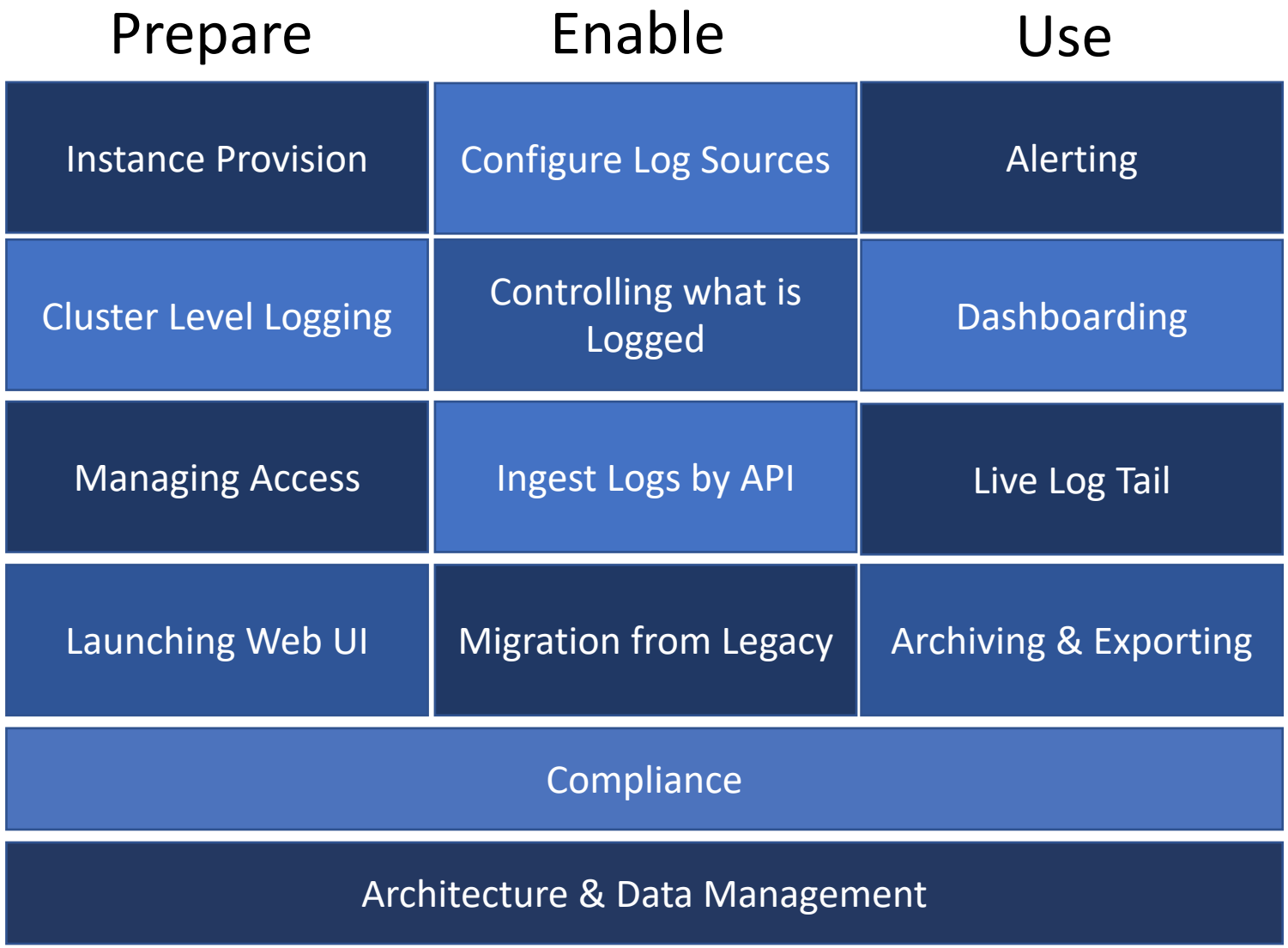
IBM services with LogDNA are located in the Cloud Navigator in Observability

And find the offerings in the IBM Cloud catalog



Topic Details

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

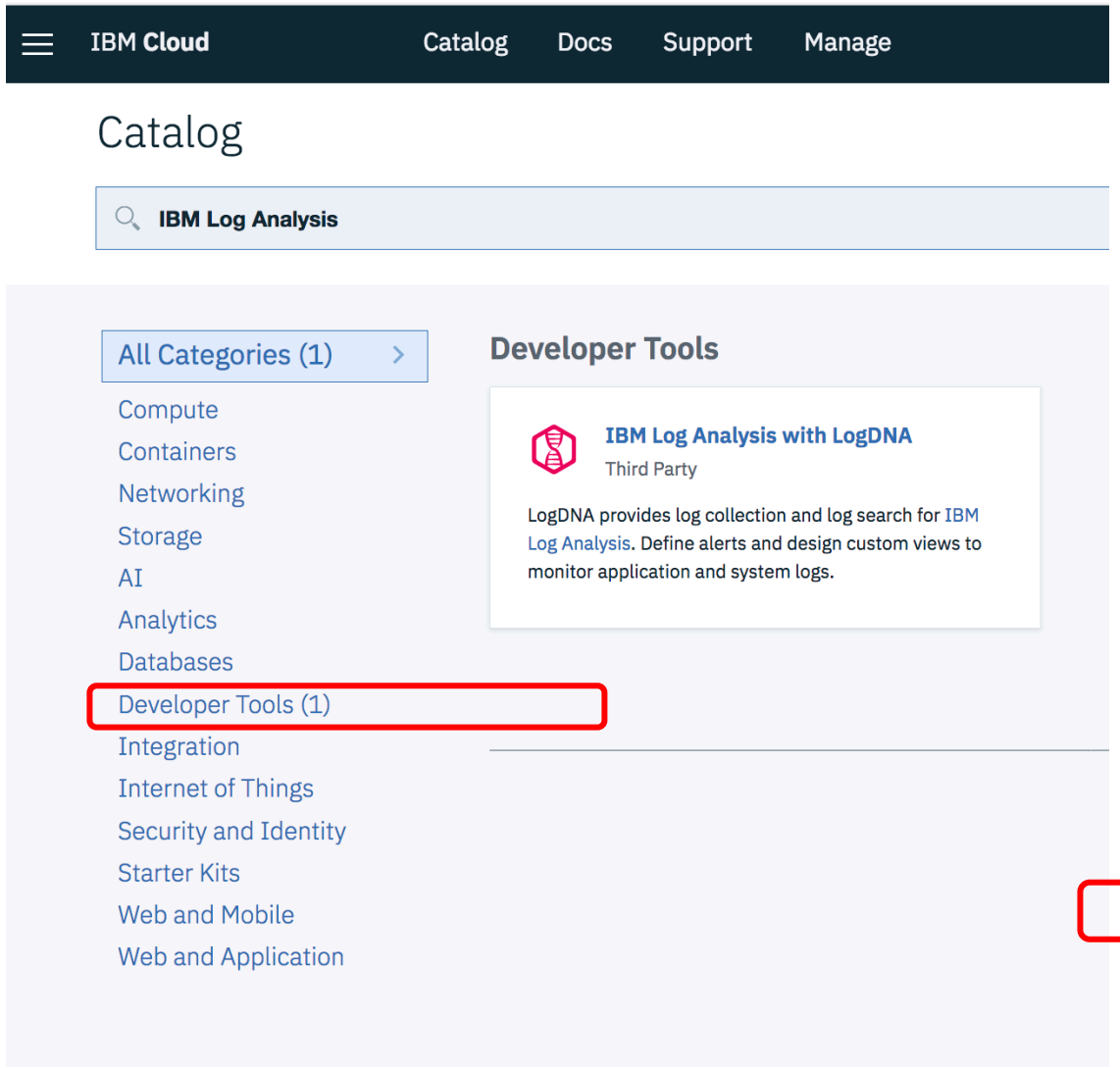


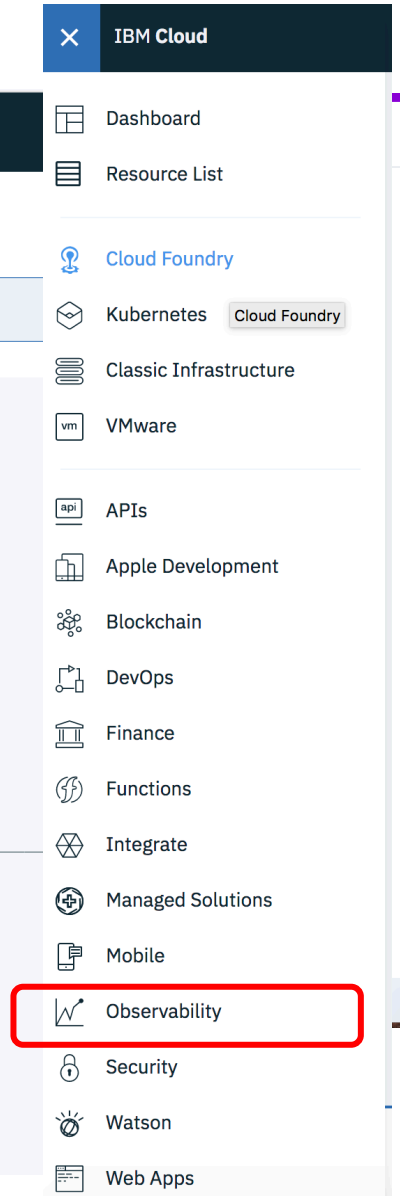
Start your journey today

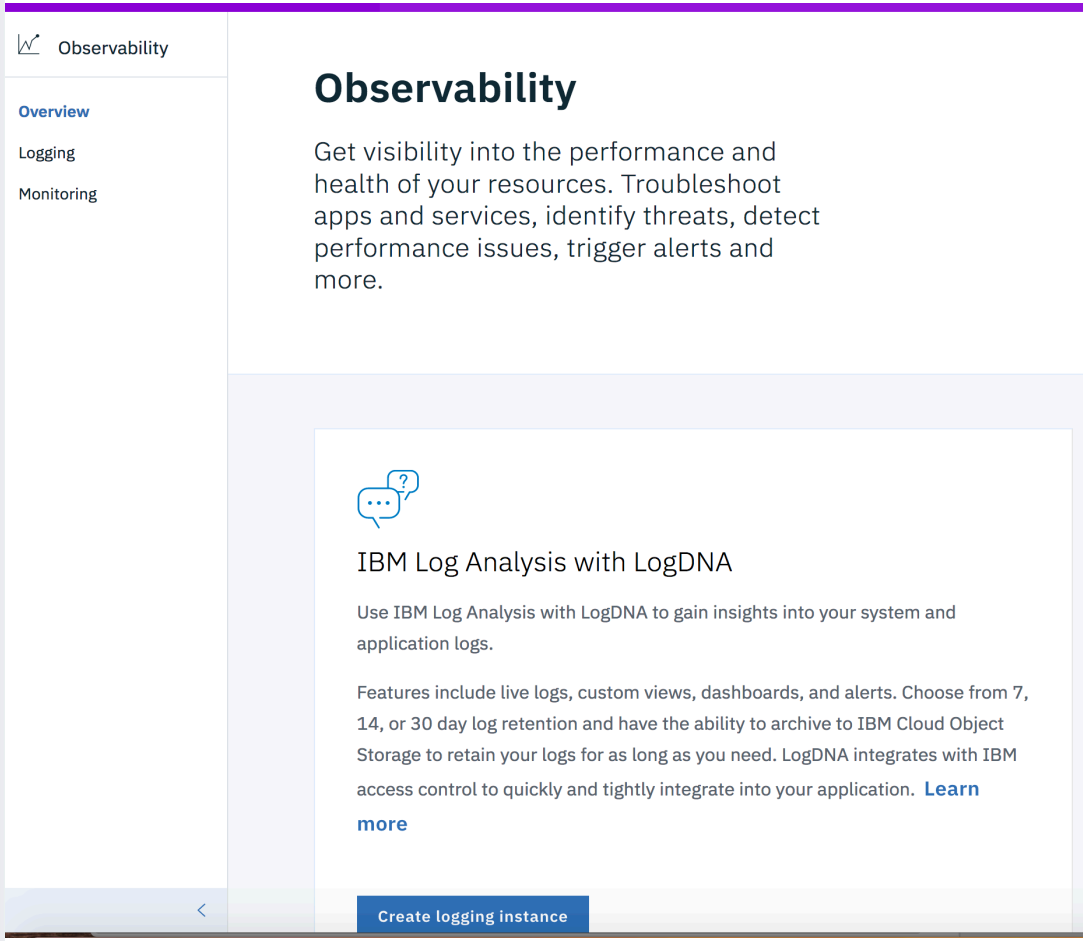
- IBM Log Analysis with LogDNA: Learn more
- Observability in IBM Cloud: Explore LogDNA from within IBM Cloud
- IBM Log Analysis with LogDNA in service catalog: Create a service instance
- Documentation

Thank you

Provisioning an instance

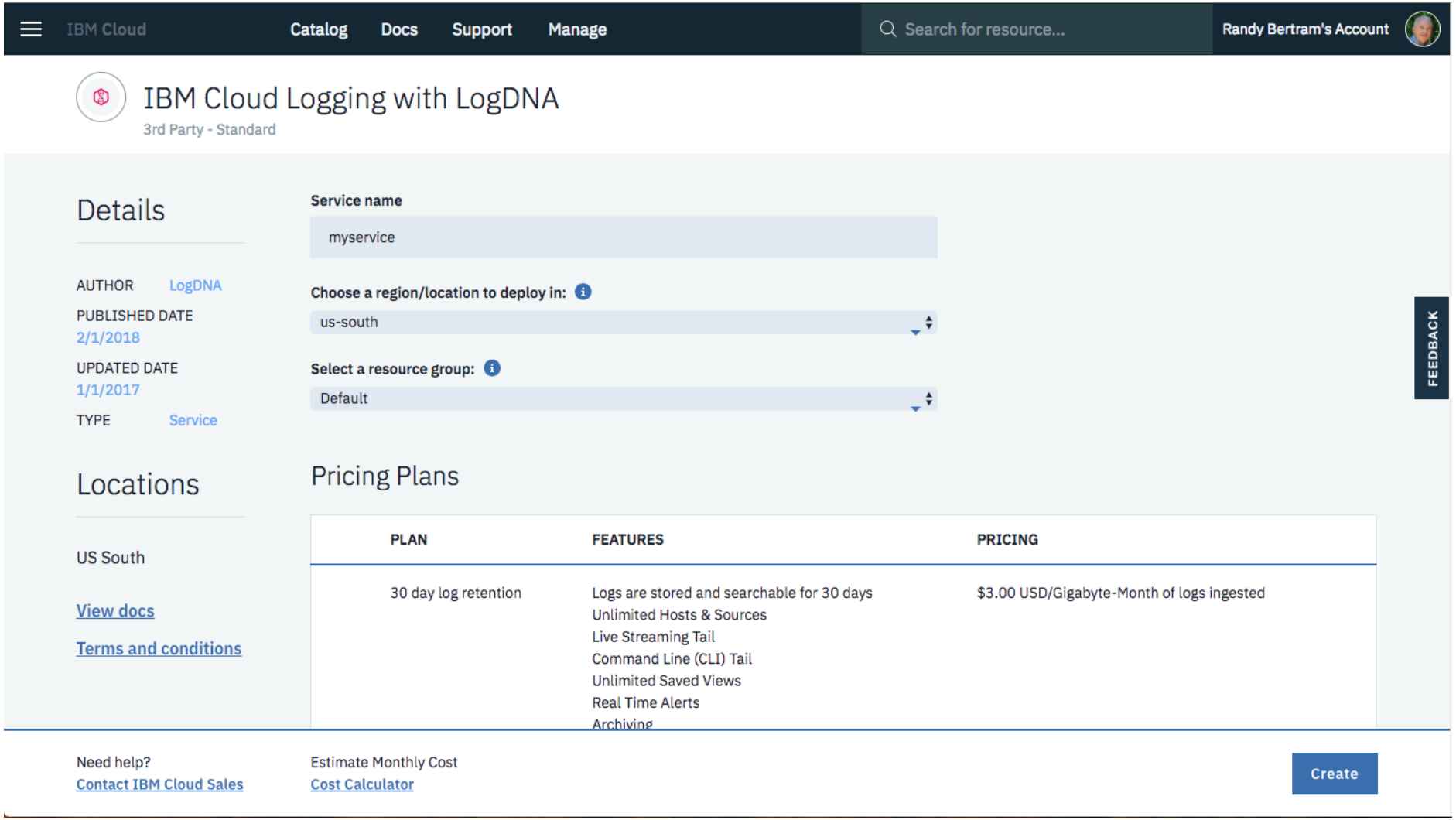






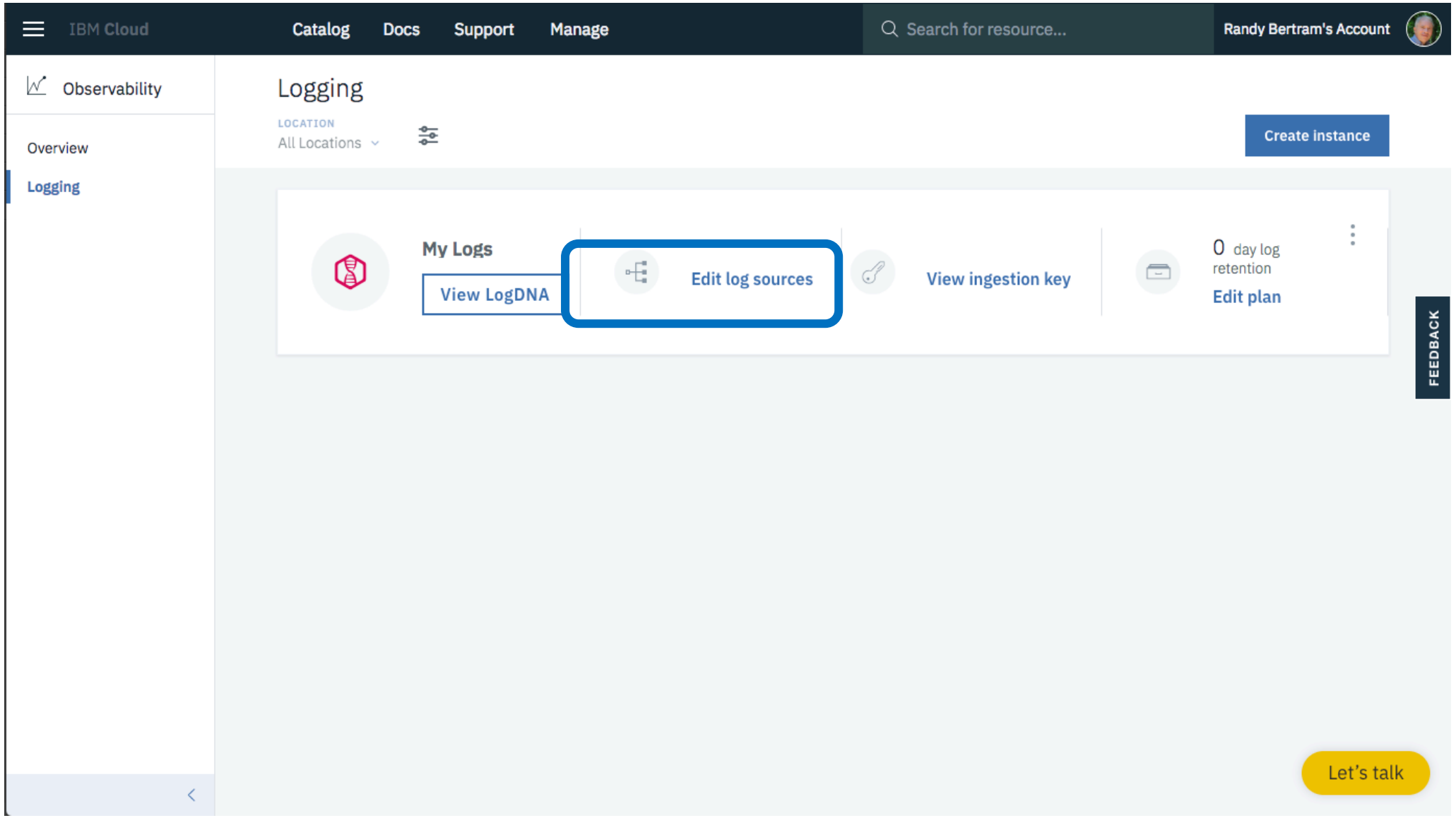
NEW AREA

Provisioning an instance

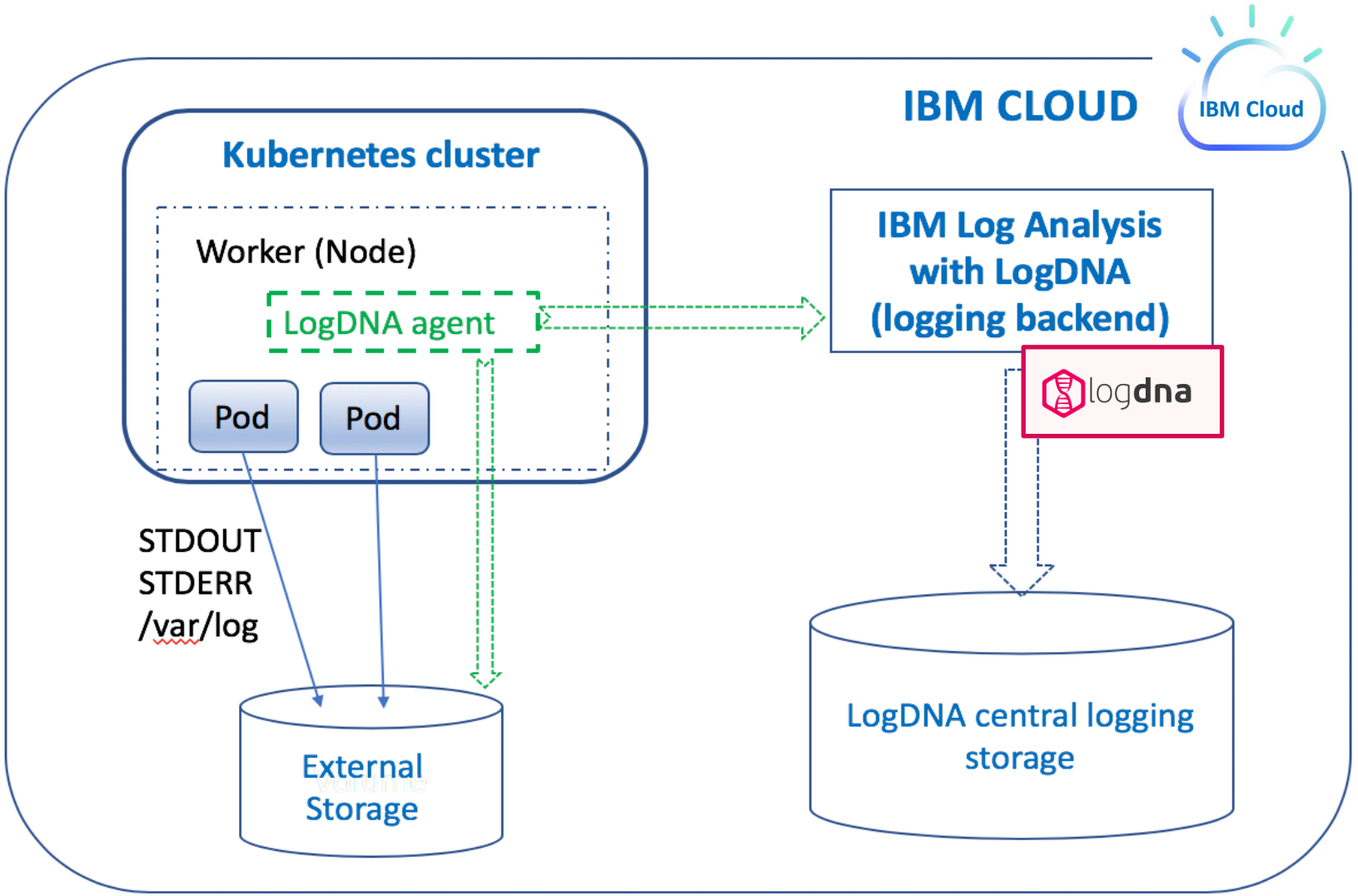


Provisioned instances

menu

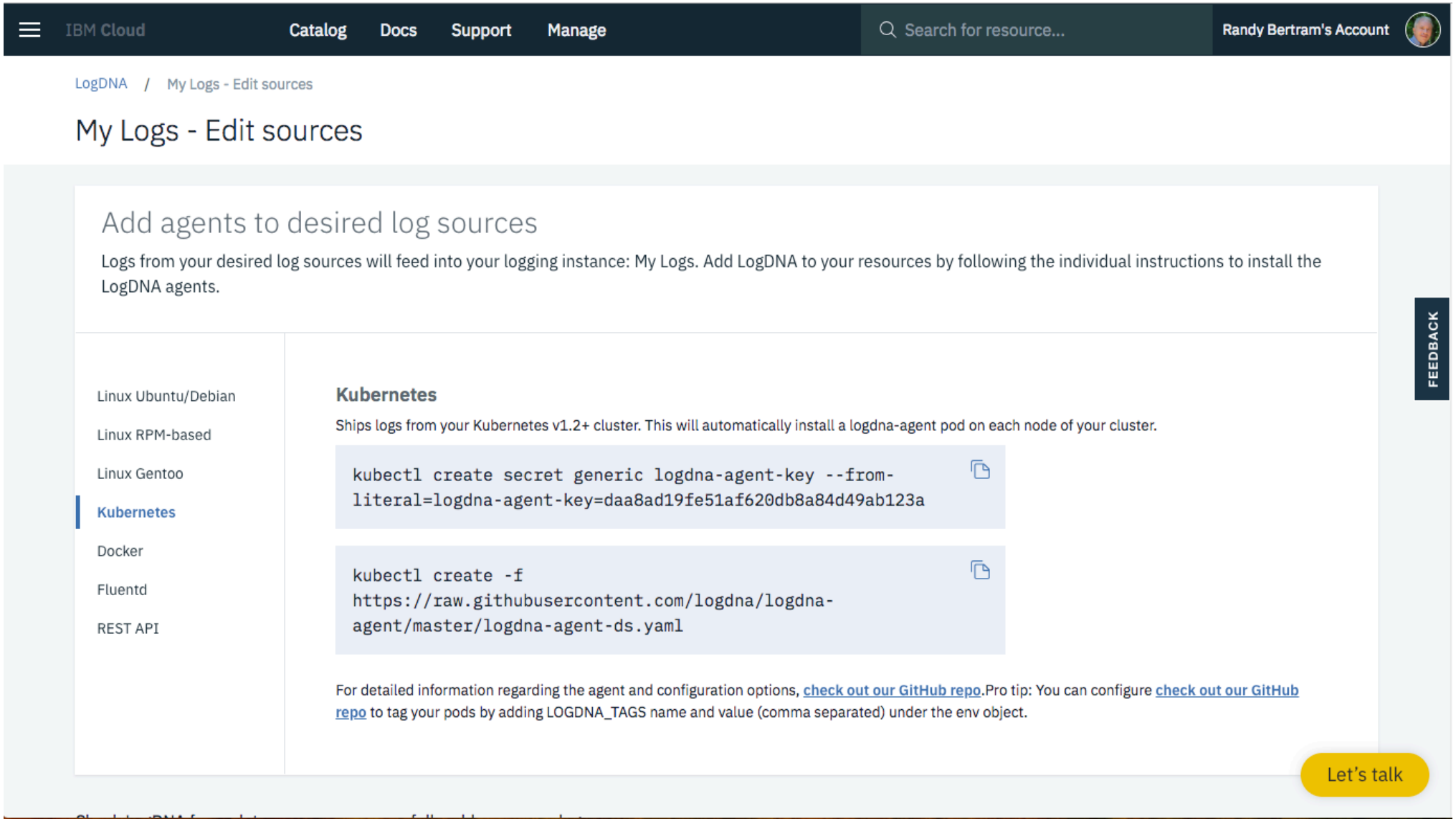


Cluster-level Logging for the IBM Cloud Kubernetes Service



Cluster-level Logging for the IBM Cloud Kubernetes Service

menu



Managing access from the IBM Cloud

menu

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:

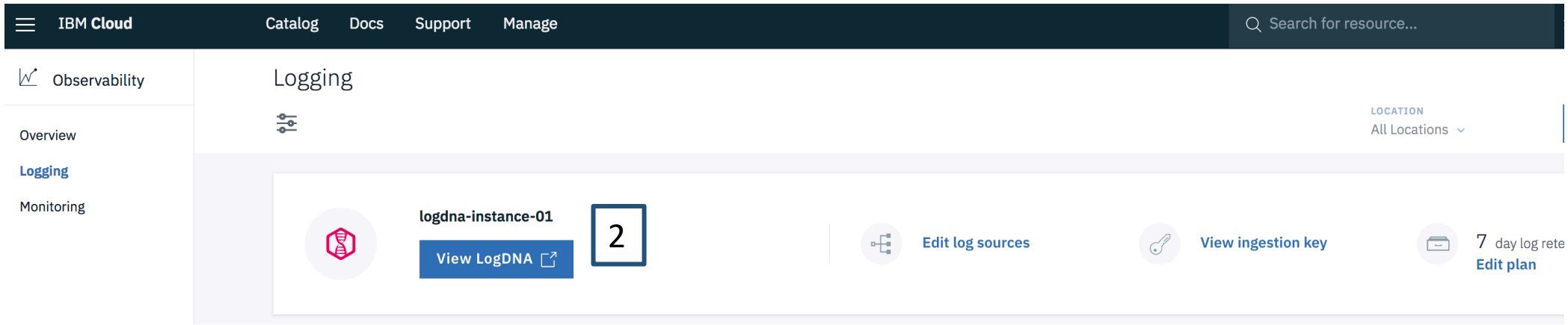
Platform actions	IBM Cloud Platform Roles
Grant other account members access to work with the service	Administrator
Provision a service instance	Administrator Editor
Delete a service instance	Administrator Editor
Create a service ID	Administrator Editor
View details of a service instance	Administrator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

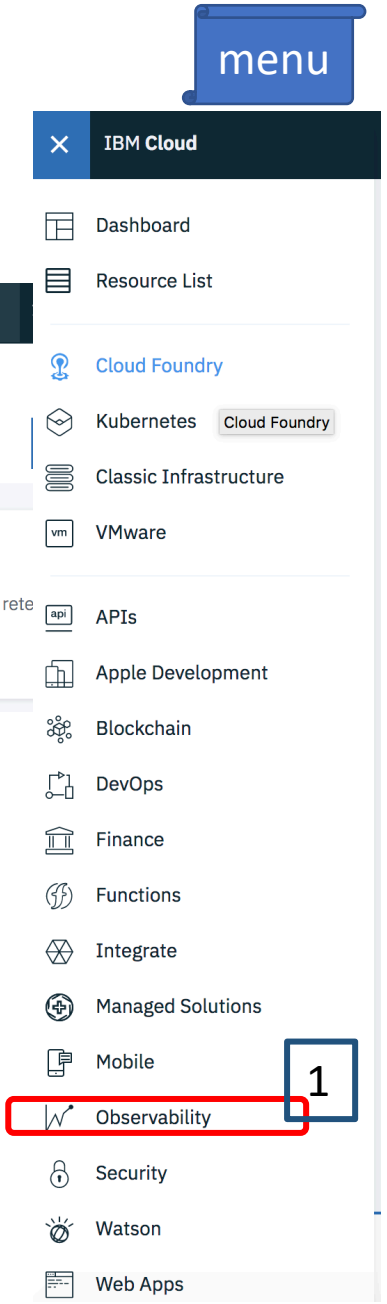
IBM Cloud service roles

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





Configuring user preferences

menu

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

Viewer Style
Viewer Options
Log Format

- [x] Muted `DEBUG` statements

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

- [ ] Show `%time` as UTC

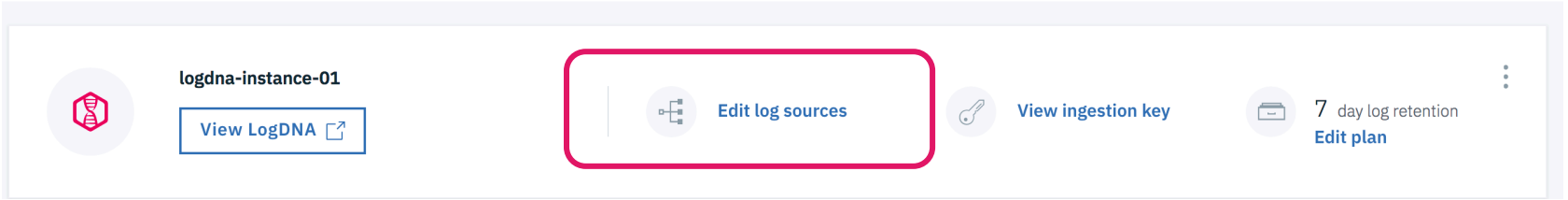
  Timestamps will be shown in UTC and timeframe searches will be done relative to UTC instead of local time.

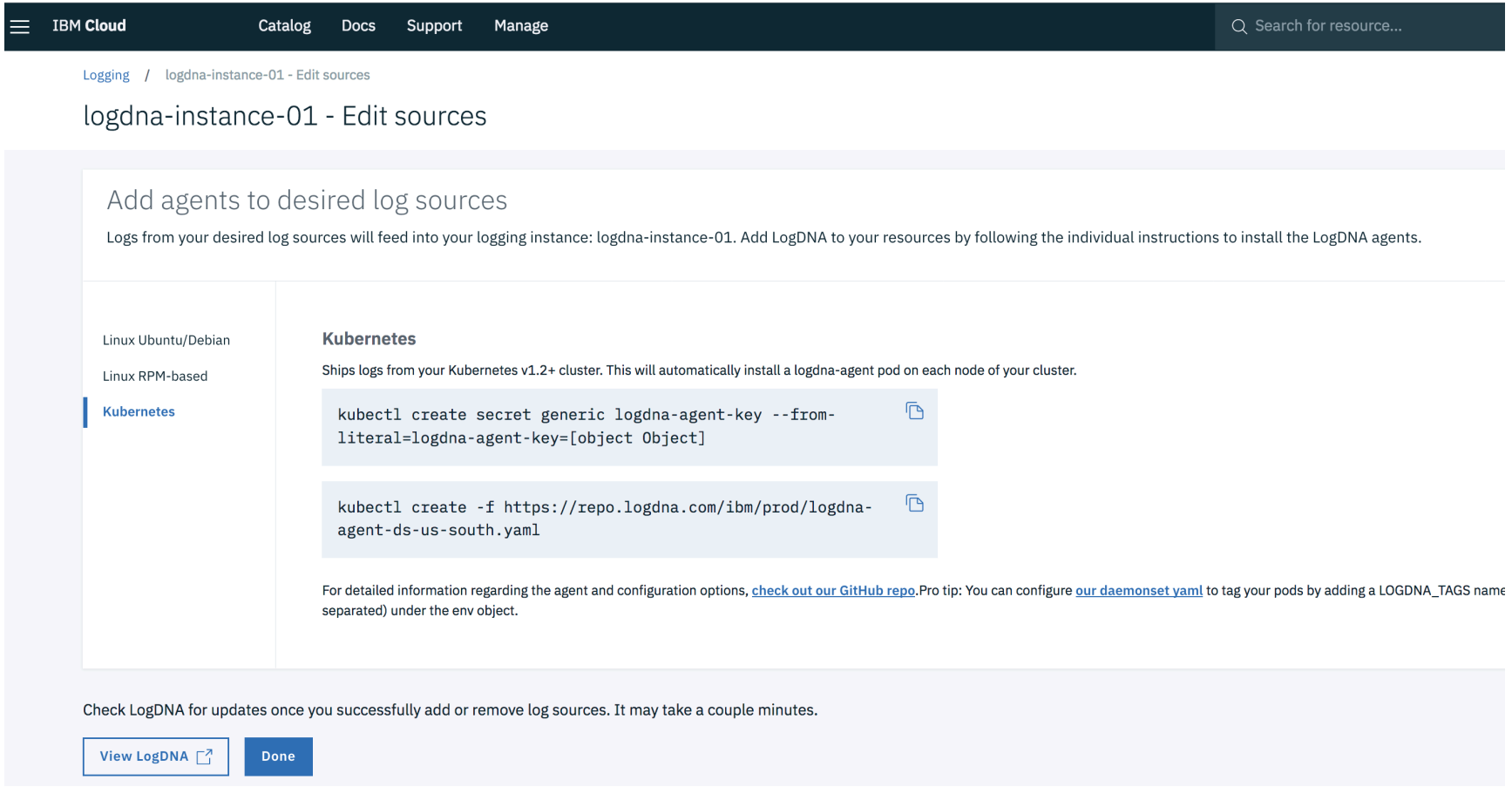
- [ ] Show raw line inside line context

  Show the original line as it was received.

Configuring log sources to send logs

menu

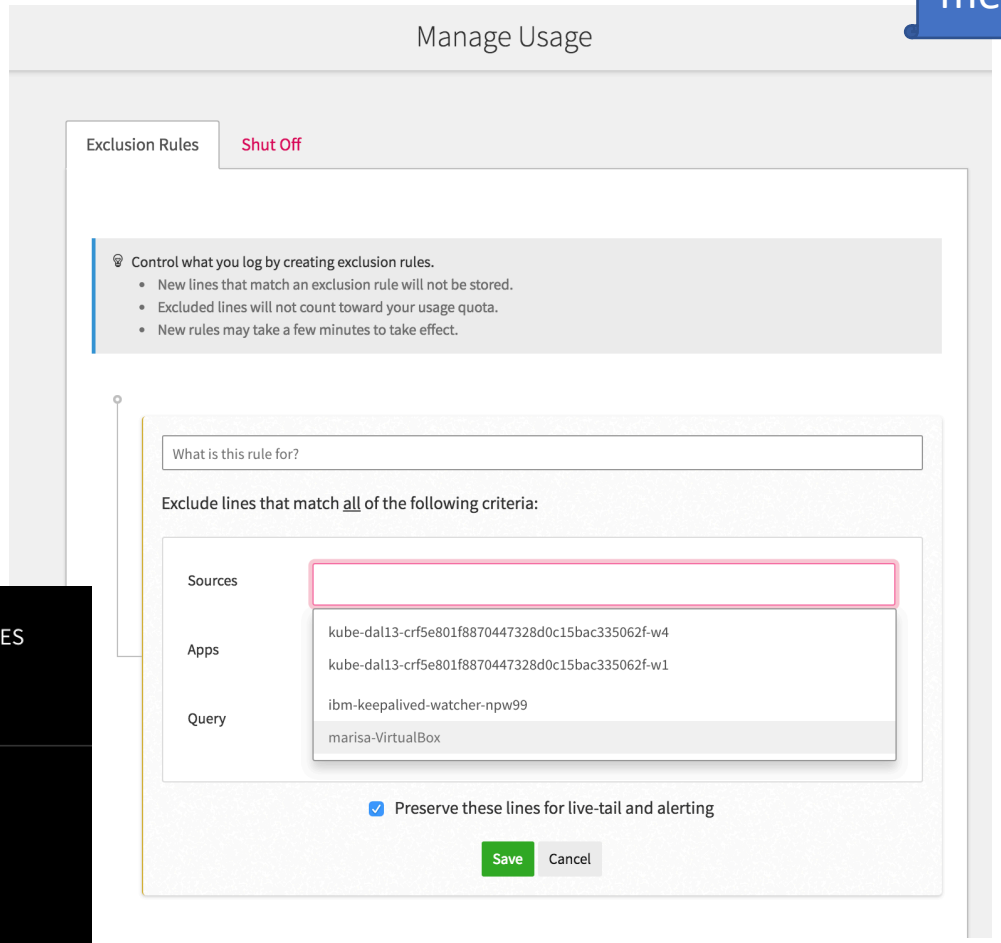




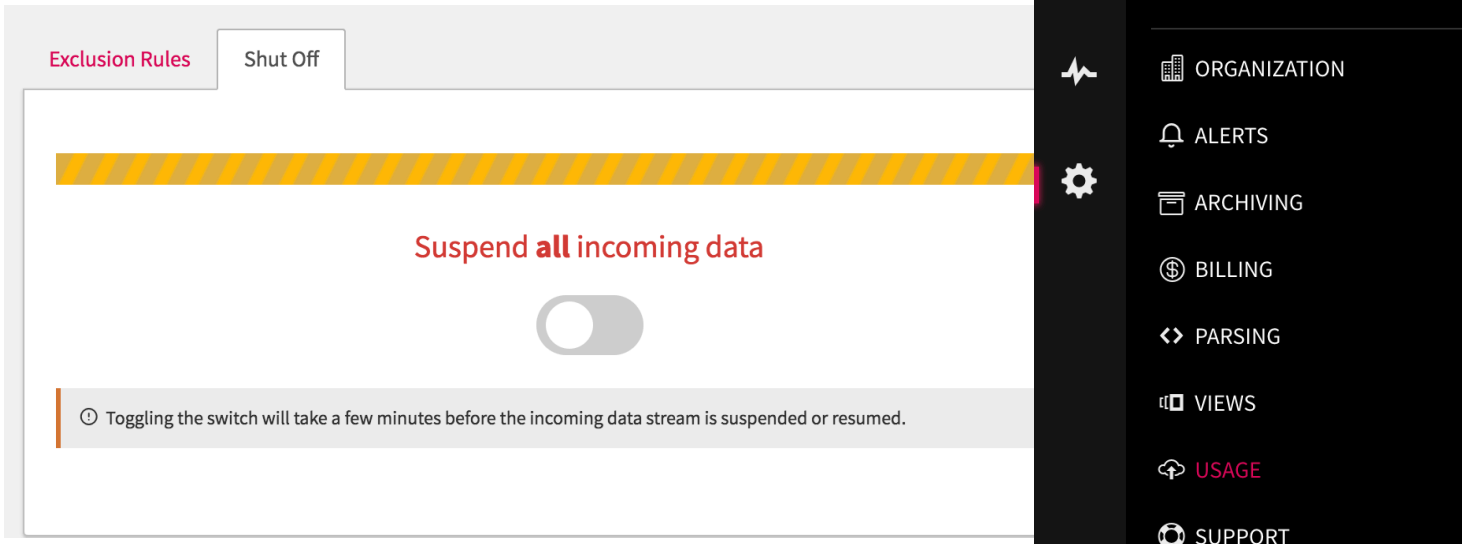
Controlling what you log

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

menu

```
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

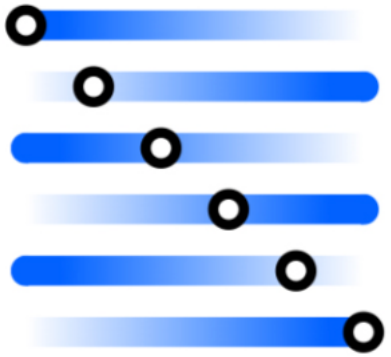
```
{
  "lines": [
    {
      "timestamp": 2018-11-02T10:53:06+00:00,
      "line":"This is my first log line.",
      "app":"myapp",
      "level": "INFO",
      "meta": {
        "customfield": {"nestedfield": "nestedvalue"}
      }
    }
  ]
}
```

```
curl "https://logs.us-south.logging.cloud.ibm.com/logs/ingest?hostname=MYHOST&now=$(date +%s)000" -u xxxxxxxxxxxxxxxxxxxxxxx: --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

menu

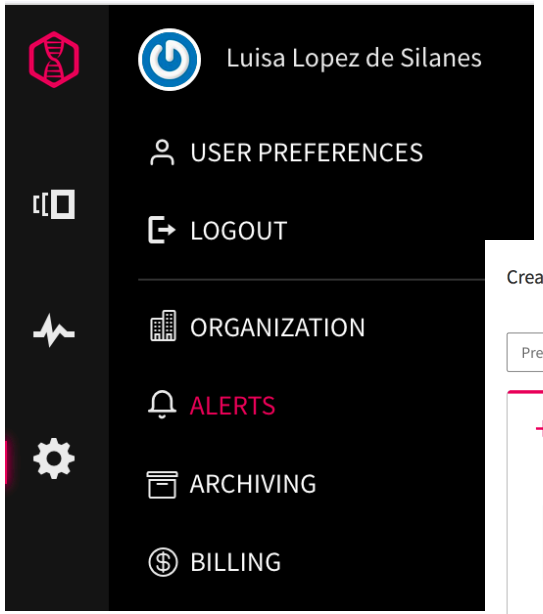
You can configure any of the following conditions for an alert:

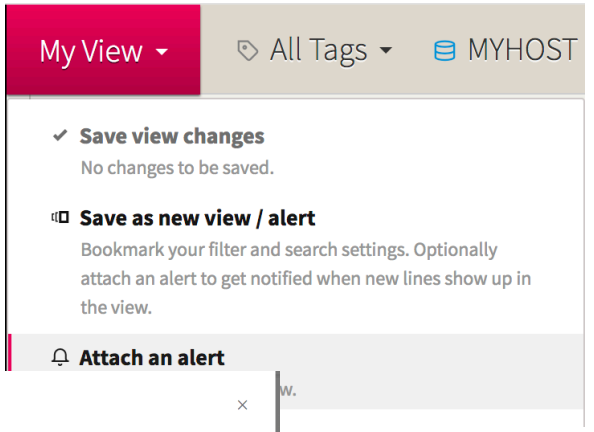
•***Time frequency***: Specify how often to trigger an alert.

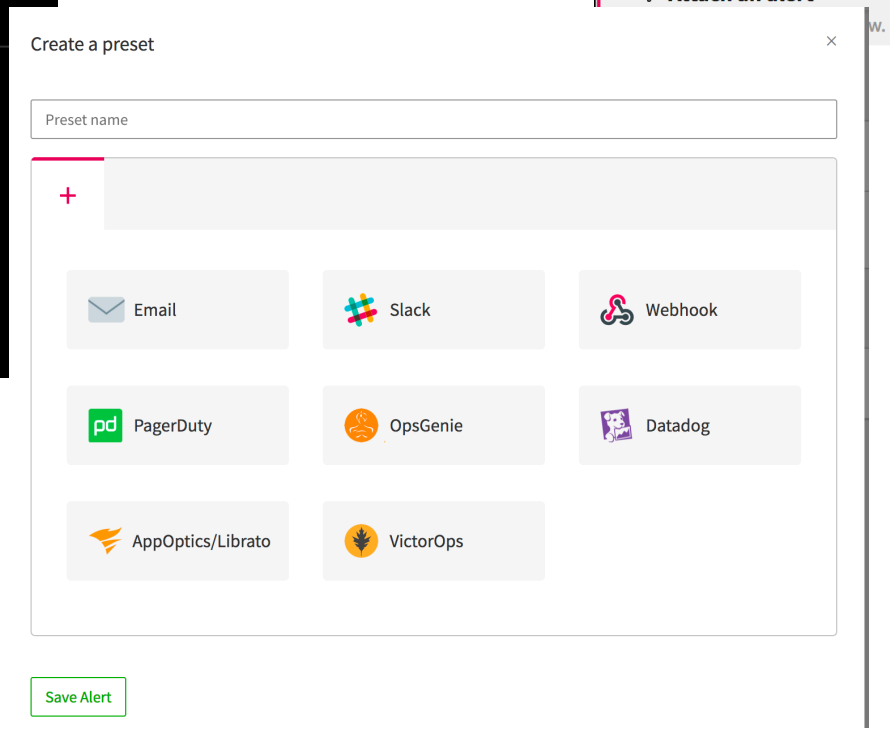
Valid values are: 30 seconds, 1 minute, 5 minutes, 15 minutes, 30 minutes, 1 hour, 6 hours, 12 hours, 24 hours

•***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

menu

Create graphs with ease.

Directly use your same search queries to generate graphs

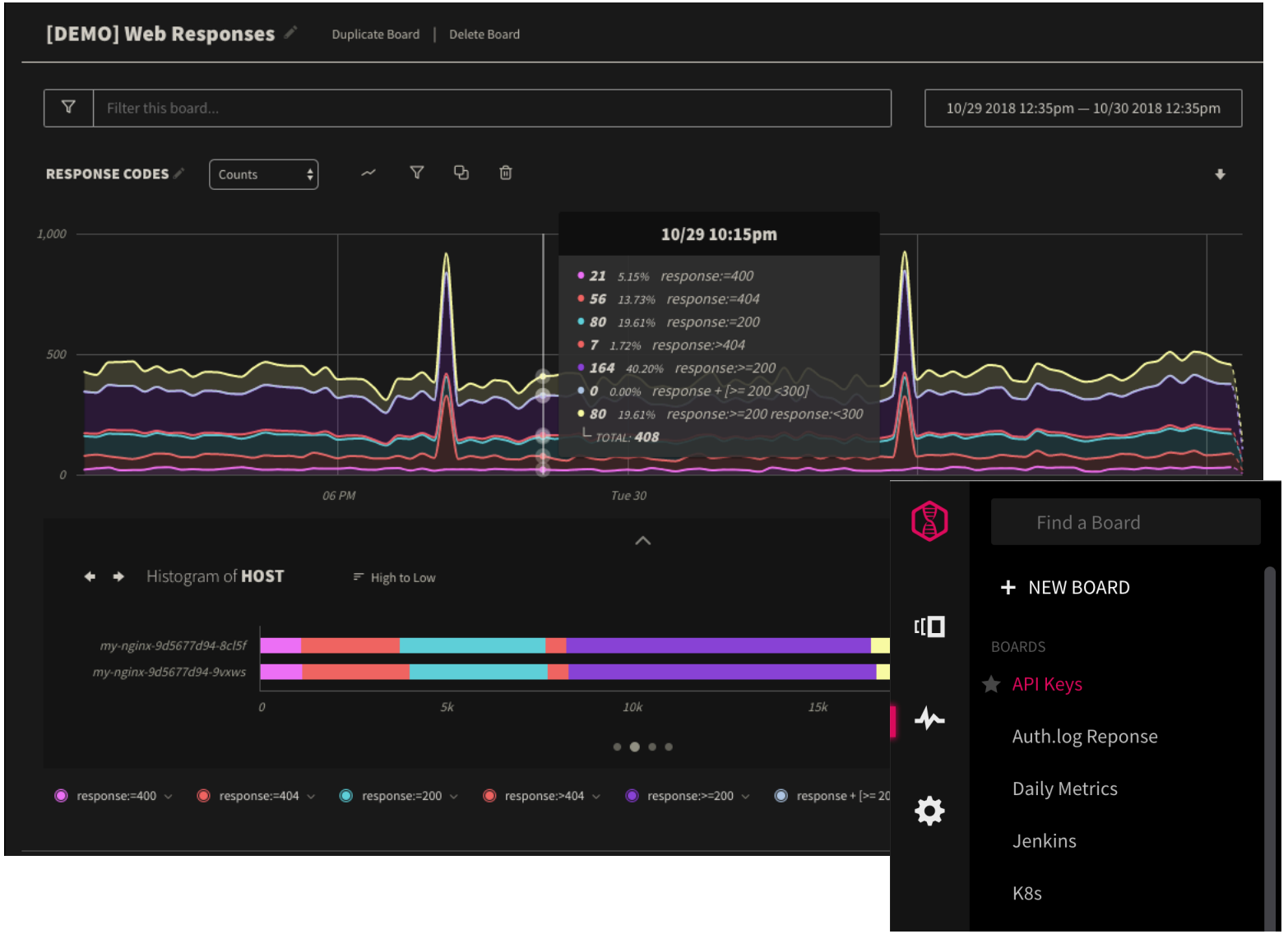
Stack additional graphs and queries to perform direct comparisons in a scoped window

Save multiple graphs into a single board

Advanced analysis capabilities

Create histograms against auto parsed fields to compare another variable

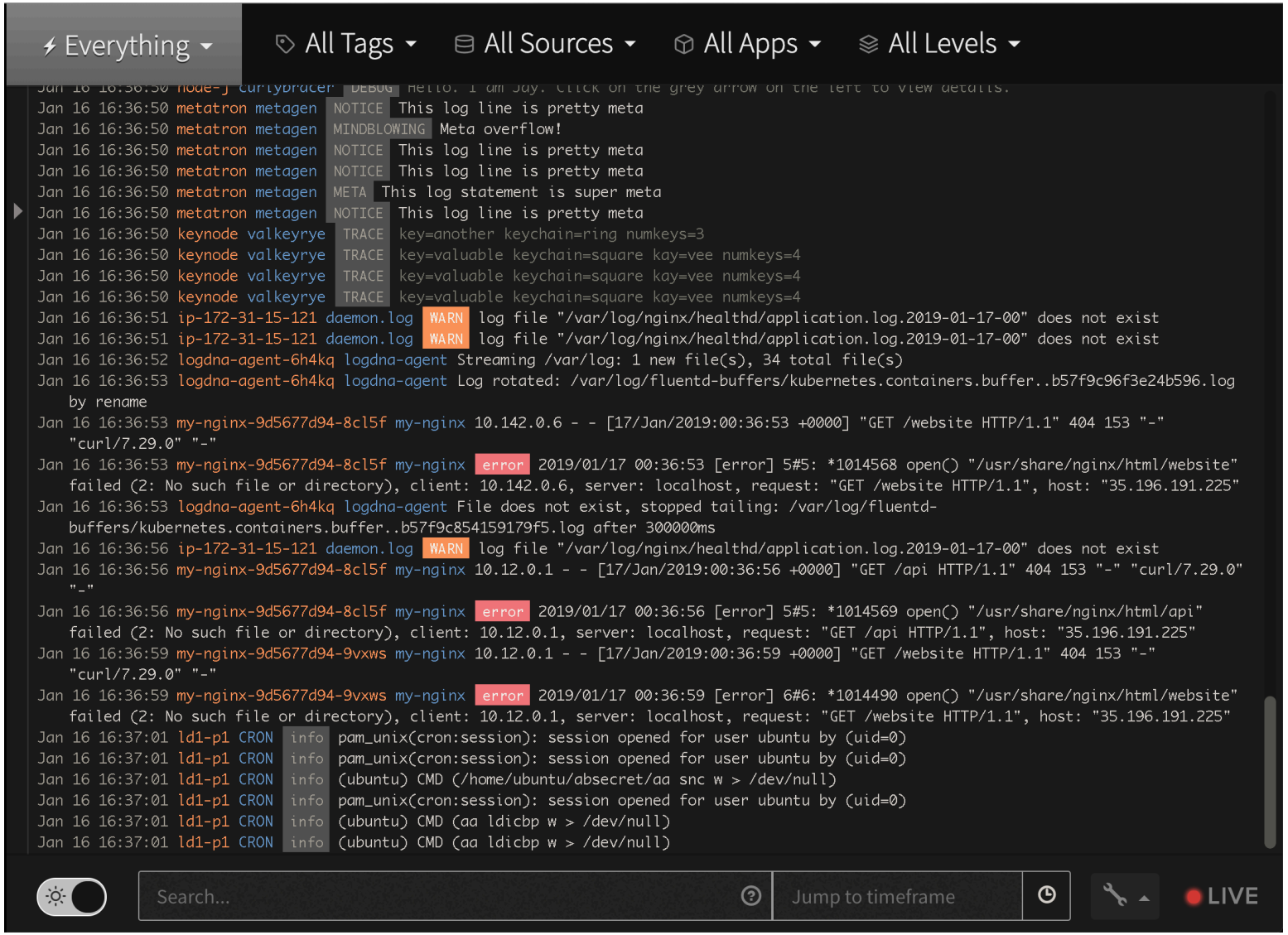
Filter and exclude parameters across a set graphs within a board



Live Log Tail

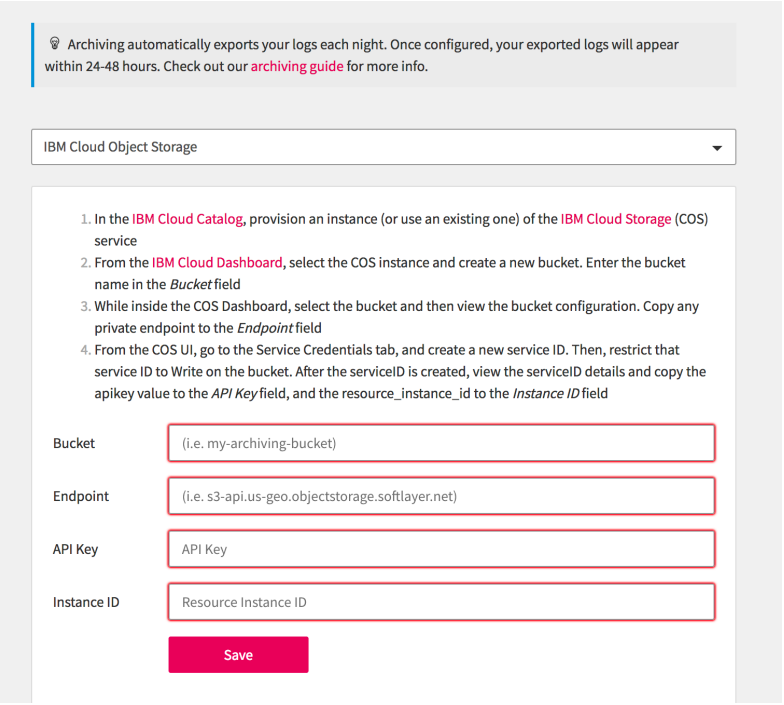
menu

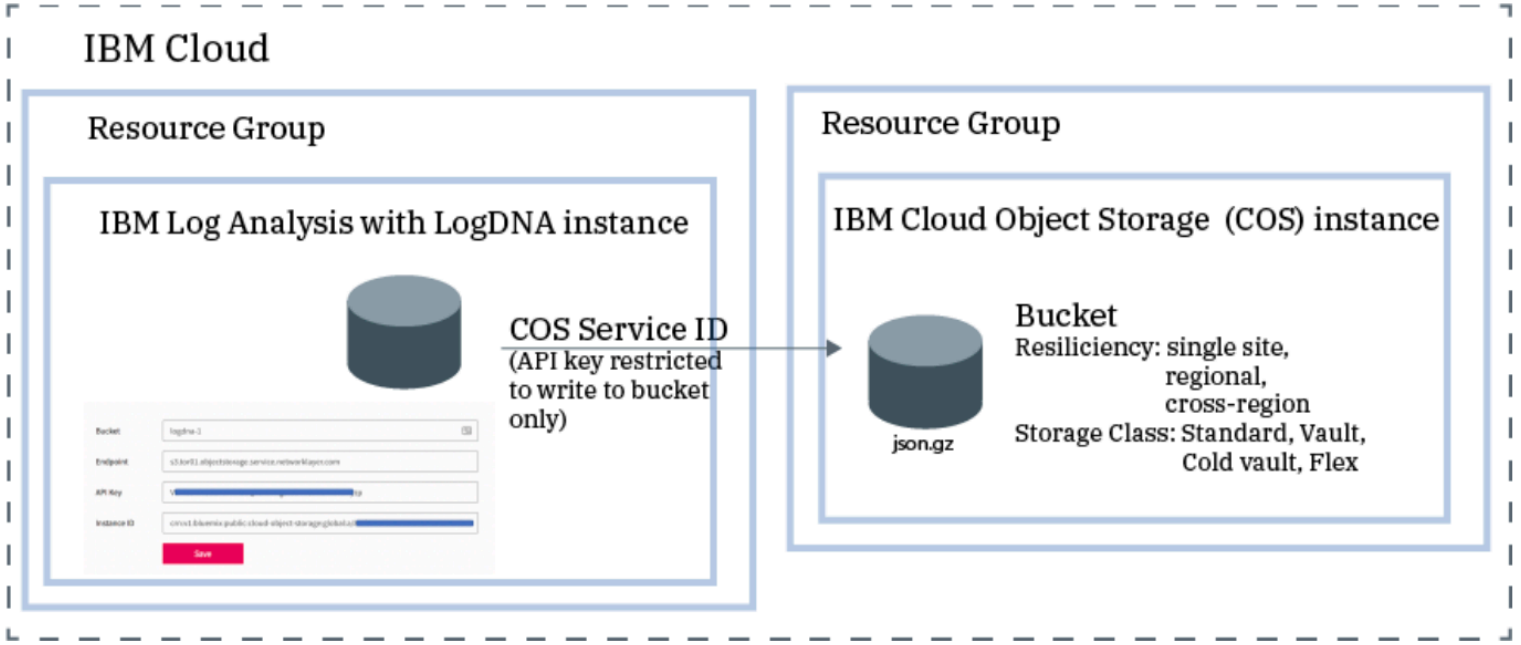
- Stream all your logs in real-time
- Use live tail to check on application and system health by watching a replay of your logs
- Average live tail latency of ~1s, Logs are parsed and streamed back out to the users while log data is being indexed for search in the backend
- Seamlessly scroll back and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



Archiving data

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.

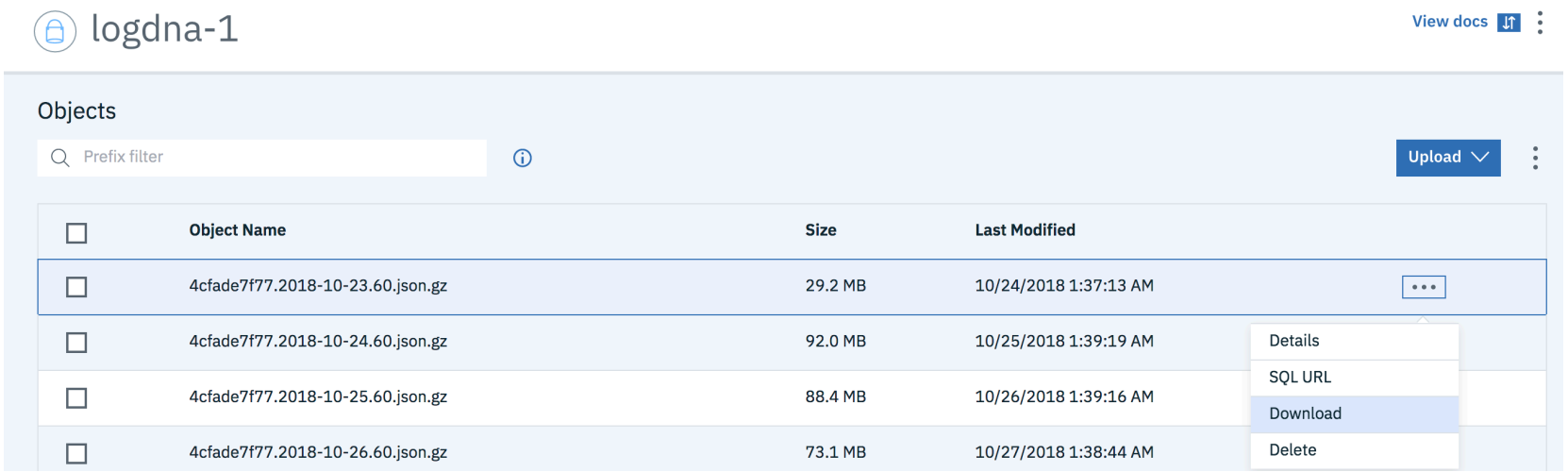
Each IBM Log Analysis with LogDNA instance has its own archiving configuration.

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.



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.

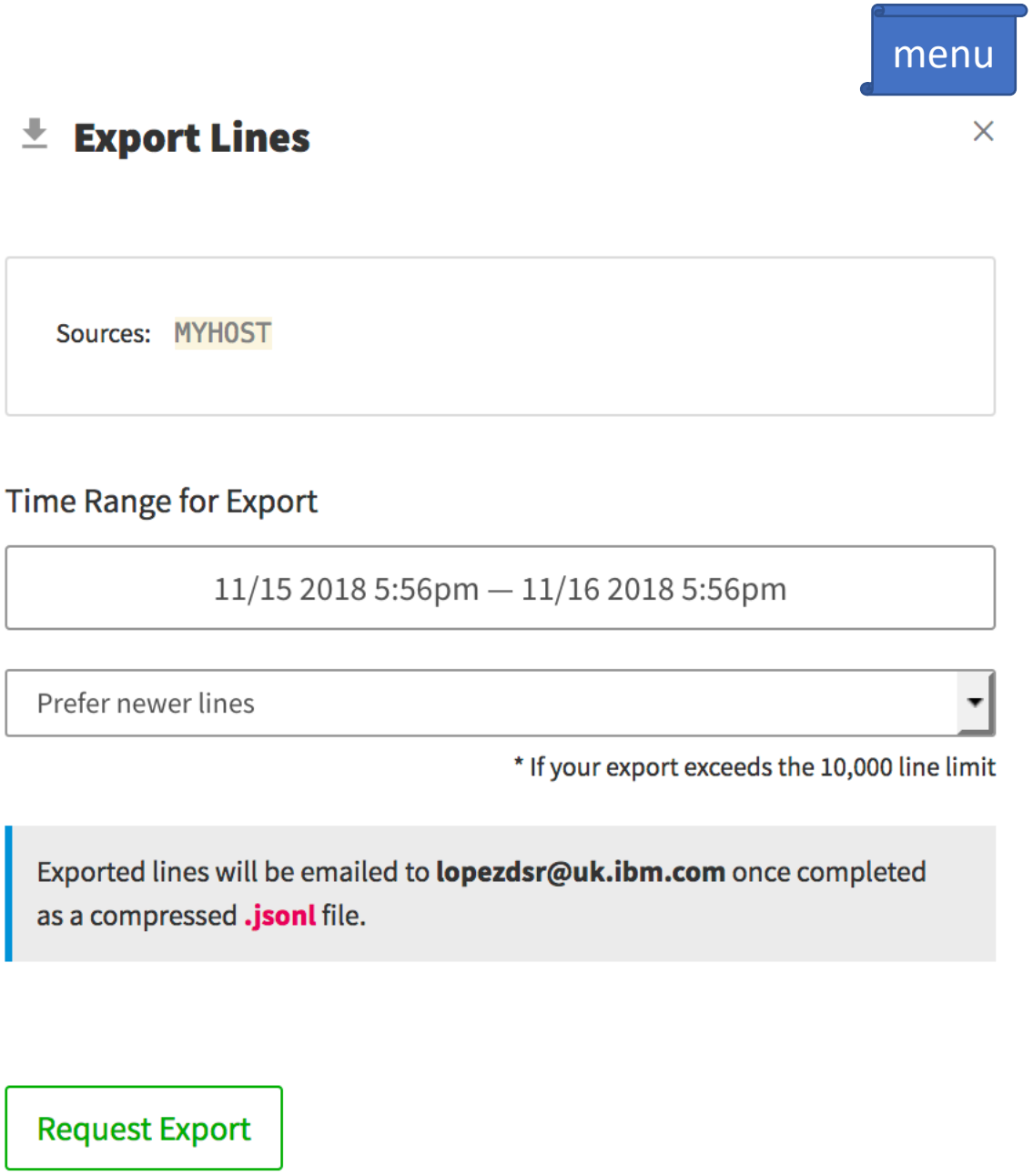
To define the set of data that you want to export, you can apply filters and searches, and specify the time range.

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.

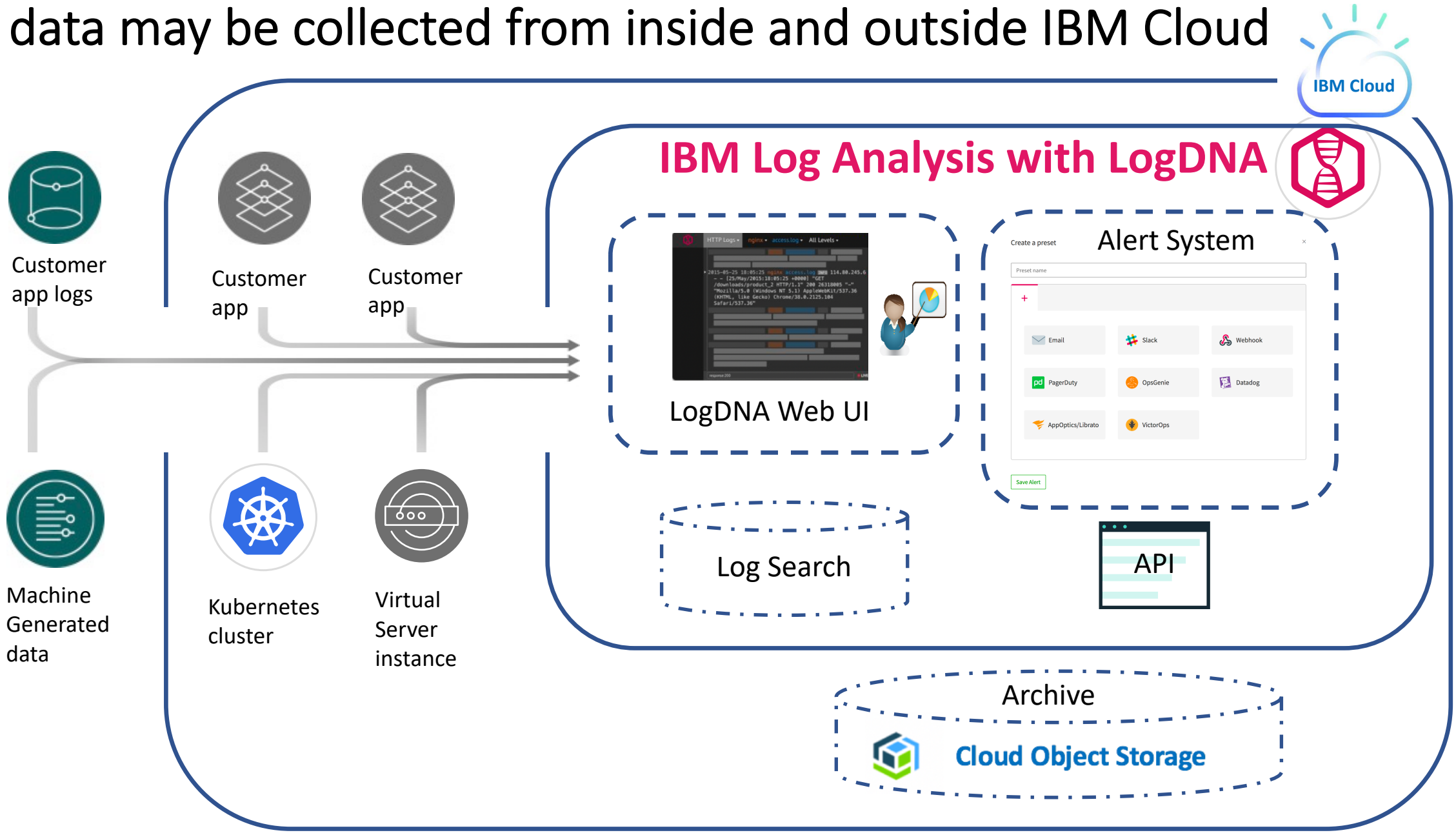
When you **export logs programmatically**, you can choose to send an email or to stream logs into your terminal.

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.



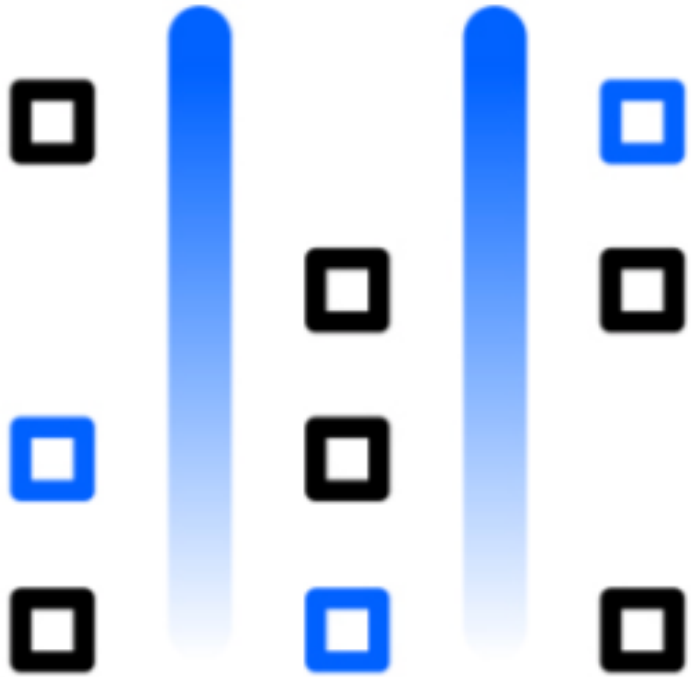
Log data may be collected from inside and outside IBM Cloud



Data Management

menu

- 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

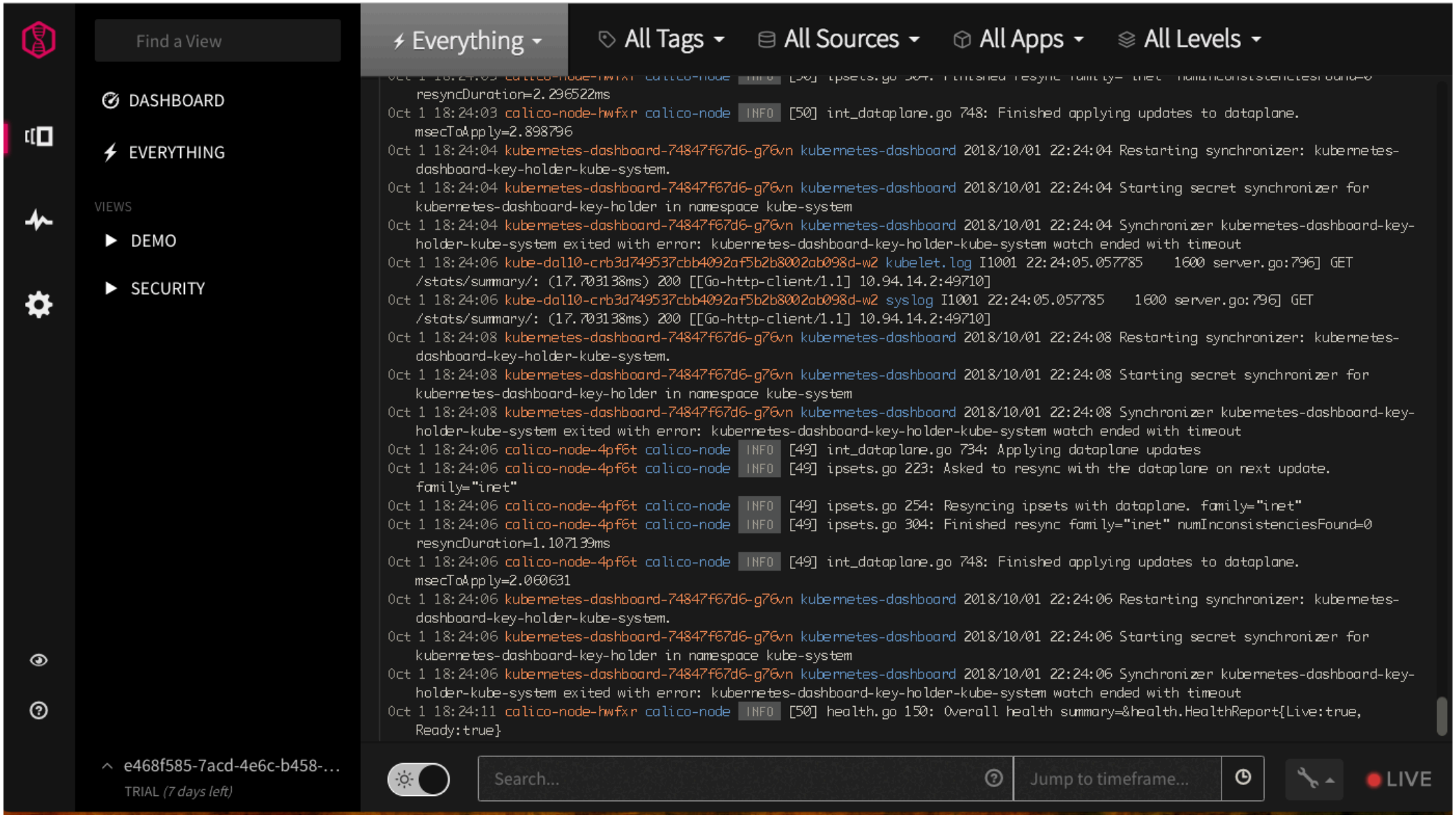


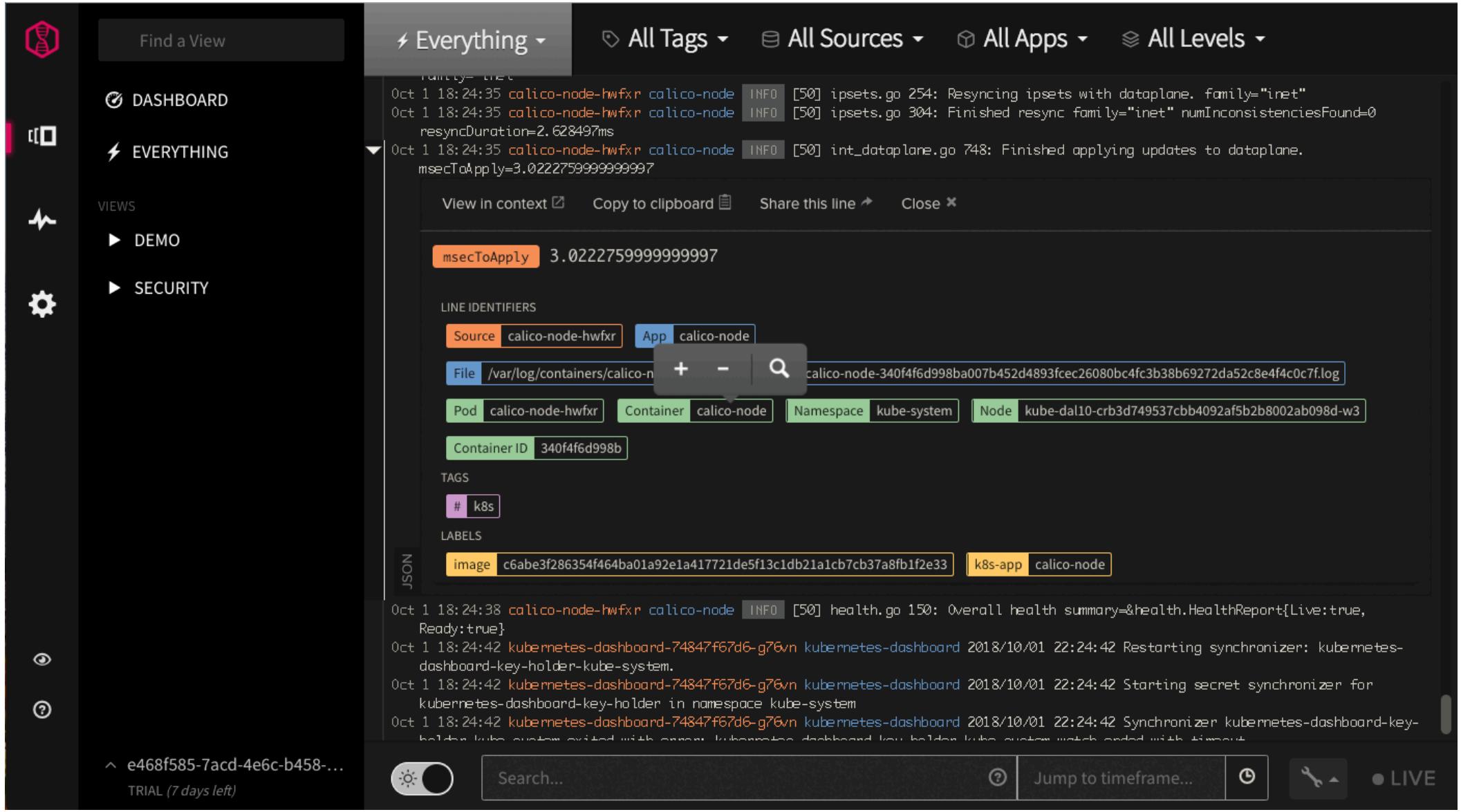
Compliance

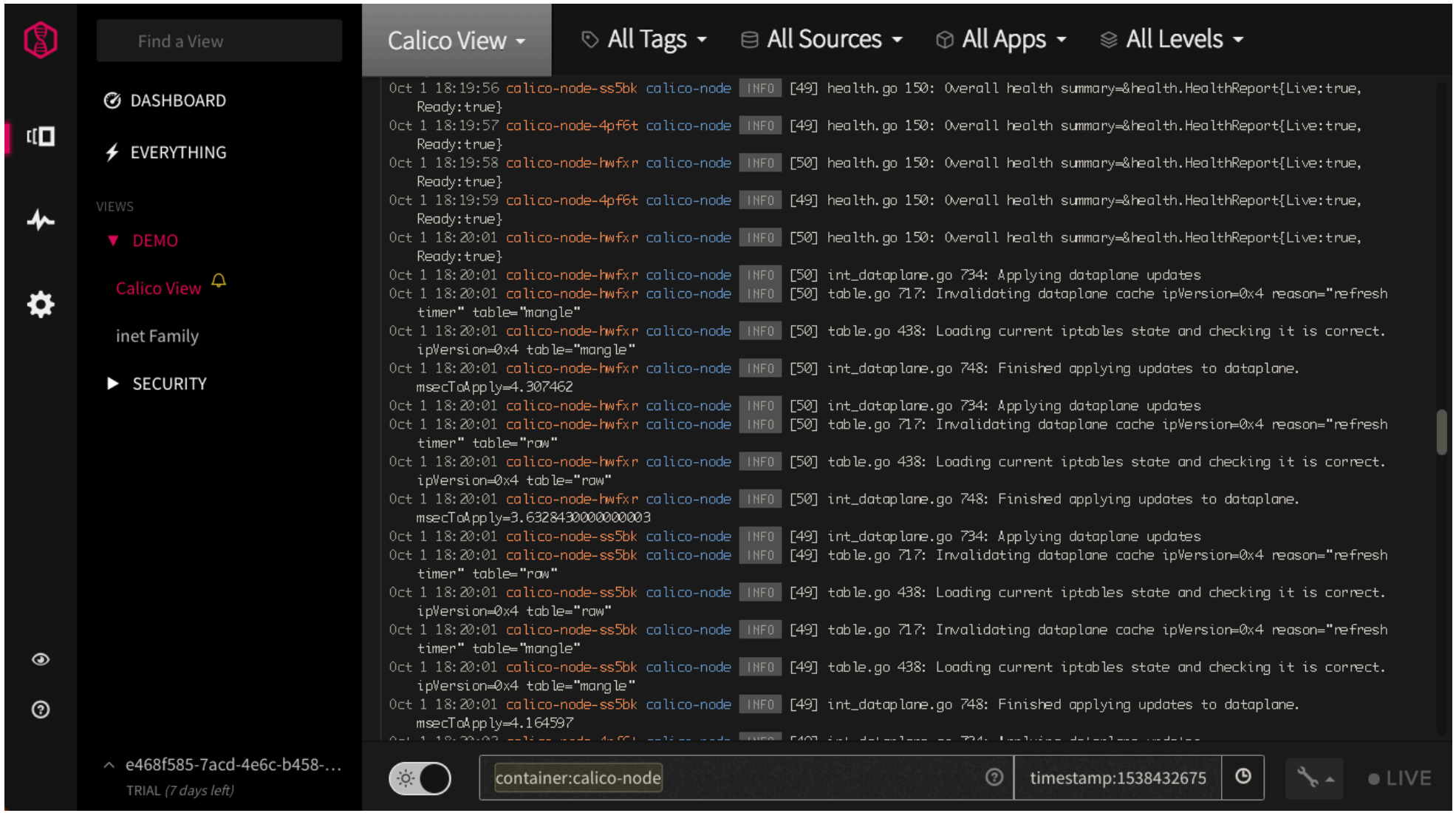
menu

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
DASHBOARD
EVERYTHING
VIEWS
DEMO
SECURITY
e468f585-7acd-4e6c-b458-...
TRIAL (7 days left)
Everything
All Tags
All Sources
All Apps
All Levels
resyncDuration=2.296522ms
Oct 1 18:24:03 calico-node-hwfxr 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-crb3d749537cbb4092af5b2b8002ab098d-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-crb3d749537cbb4092af5b2b8002ab098d-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-hwfxr calico-node INFO [50] health.go 150: Overall health summary=&health.HealthReport{Live:true, Ready:true}
Search...
Jump to timeframe...
LIVE


Find a View
DASHBOARD
EVERYTHING
VIEWS
DEMO
SECURITY
Everything
All Tags
All Sources
All Apps
All Levels
Oct 1 18:24:35 calico-node-hwfxr calico-node INFO [50] ipsets.go 254: Resyncing ipsets with dataplane. family="inet"
Oct 1 18:24:35 calico-node-hwfxr calico-node INFO [50] ipsets.go 304: Finished resync family="inet" numInconsistenciesFound=0 resyncDuration=2.628497ms
Oct 1 18:24:35 calico-node-hwfxr 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-hwfxr
App calico-node
File /var/log/containers/calico-n
calico-node-340f4f6d998ba007b452d4893fcec26080bc4fc3b38b69272da52c8e4f4c0c7f.log
Pod calico-node-hwfxr
Container calico-node
Namespace kube-system
Node kube-dal10-crb3d749537cbb4092af5b2b8002ab098d-w3
Container ID 340f4f6d998b
TAGS
k8s
LABELS
image c6abe3f286354f464ba01a92e1a417721de5f13c1db21a1cb7cb37a8fb1f2e33
k8s-app calico-node
JSON
Oct 1 18:24:38 calico-node-hwfxr 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-
e468f585-7acd-4e6c-b458-...
TRIAL (7 days left)
Search...
Jump to timeframe...
LIVE


Find a View
DASHBOARD
EVERYTHING
VIEWS
DEMO
Calico View
inet Family
SECURITY
e468f585-7acd-4e6c-b458-...
TRIAL (7 days left)
Calico View
All Tags
All Sources
All Apps
All Levels
Oct 1 18:19:56 calico-node-ss5bk calico-node INFO [49] health.go 150: Overall health summary=&health.HealthReport{Live:true, Ready:true}
Oct 1 18:19:57 calico-node-4pf6t calico-node INFO [49] health.go 150: Overall health summary=&health.HealthReport{Live:true, Ready:true}
Oct 1 18:19:58 calico-node-hwfxr calico-node INFO [50] health.go 150: Overall health summary=&health.HealthReport{Live:true, Ready:true}
Oct 1 18:19:59 calico-node-4pf6t calico-node INFO [49] health.go 150: Overall health summary=&health.HealthReport{Live:true, Ready:true}
Oct 1 18:20:01 calico-node-hwfxr calico-node INFO [50] health.go 150: Overall health summary=&health.HealthReport{Live:true, Ready:true}
Oct 1 18:20:01 calico-node-hwfxr calico-node INFO [50] int_dataplane.go 734: Applying dataplane updates
Oct 1 18:20:01 calico-node-hwfxr calico-node INFO [50] table.go 717: Invalidating dataplane cache ipVersion=0x4 reason="refresh timer" table="mangle"
Oct 1 18:20:01 calico-node-hwfxr calico-node INFO [50] table.go 438: Loading current iptables state and checking it is correct. ipVersion=0x4 table="mangle"
Oct 1 18:20:01 calico-node-hwfxr calico-node INFO [50] int_dataplane.go 748: Finished applying updates to dataplane. msecToApply=4.307462
Oct 1 18:20:01 calico-node-hwfxr calico-node INFO [50] int_dataplane.go 734: Applying dataplane updates
Oct 1 18:20:01 calico-node-hwfxr calico-node INFO [50] table.go 717: Invalidating dataplane cache ipVersion=0x4 reason="refresh timer" table="raw"
Oct 1 18:20:01 calico-node-hwfxr calico-node INFO [50] table.go 438: Loading current iptables state and checking it is correct. ipVersion=0x4 table="raw"
Oct 1 18:20:01 calico-node-hwfxr calico-node INFO [50] int_dataplane.go 748: Finished applying updates to dataplane. msecToApply=3.6328430000000003
Oct 1 18:20:01 calico-node-ss5bk calico-node INFO [49] int_dataplane.go 734: Applying dataplane updates
Oct 1 18:20:01 calico-node-ss5bk calico-node INFO [49] table.go 717: Invalidating dataplane cache ipVersion=0x4 reason="refresh timer" table="raw"
Oct 1 18:20:01 calico-node-ss5bk calico-node INFO [49] table.go 438: Loading current iptables state and checking it is correct. ipVersion=0x4 table="raw"
Oct 1 18:20:01 calico-node-ss5bk calico-node INFO [49] table.go 717: Invalidating dataplane cache ipVersion=0x4 reason="refresh timer" table="mangle"
Oct 1 18:20:01 calico-node-ss5bk calico-node INFO [49] table.go 438: Loading current iptables state and checking it is correct. ipVersion=0x4 table="mangle"
Oct 1 18:20:01 calico-node-ss5bk calico-node INFO [49] int_dataplane.go 748: Finished applying updates to dataplane. msecToApply=4.164597
container:calico-node
timestamp:1538432675
LIVE