

Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 71
CS Practical 5

Scenario : You are part of a DevOps team managing a large-scale, production-grade Kubernetes cluster hosting critical microservices. The current logging solution is inadequate, making it difficult to monitor, troubleshoot, and analyze application performance.

1. Your first task is to learn how to add and configure the Ingress component in Kubernetes
2. Following this, you'll implement a robust logging solution to gain access to various logs, including worker, pod, app, and network logs, for better monitoring.

Steps and Screenshots :

The screenshot shows the IBM Cloud Kubernetes dashboard for a cluster named 'mycluster-dal10-b3c.4x16-group3'. The 'Ingress' tab is selected in the sidebar. On the main page, the 'Domains' tab is active, displaying a table of domain records. One row is highlighted with a red box, showing the domain 'mycluster-dal10-b3c-4x16-3e4769f510db5aaf1089354e49621b41-0000.au-syd.containers.appdomain.cloud' with a status of 'Default'. Below the table, there is a button labeled 'copy ingress ID'.

Domain	Records	Status
mycluster-dal10-b3c-4x16-3e4769f510db5aaf1089354e49621b41-0000.au-syd.containers.appdomain.cloud	159.23.68.234	OK

Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 71
CS Practical 5

Cluster ID: cr3cpfc0m882o64nbq0 Version: 1.30.4_1534 Infrastructure: Classic Master location: Sydney

Worker zones: Sydney 01 Created: 8/22/2024, 10:59 AM Resource group: default Image security enforcement: Enable

Worker node health: 1 total worker nodes (100% Normal)

Networking: Service endpoint URL (Public enabled, Copy link), Ingress secrets instance (None, Manage), Ingress subdomain: mycluster-dal10-b3c-4x16-3e4769f510db5aafl089354e49621b41-0000.au-syd.containers.appdomain.cloud, Ingress ALB automatic updates (Enabled, Manage).

Integrations: Logging, Monitoring, Cluster encryption.

1. Create ingress file for previous project

```
apiVersion: networking.k8s.io/v1
kind: Ingress
metadata:
  name: yashlani-prjkt-ingress
  namespace: default
  annotations:
    nginx.ingress.kubernetes.io/from-to-www-redirect: "true"
    nginx.ingress.kubernetes.io/rewrite-target: "/"
    nginx.ingress.kubernetes.io/ssl-redirect: "true"
spec:
  ingressClassName: public-iks-k8s-nginx
  tls:
```

Name - Yash Lakhtariya

Enrollment number - 21162101012

Branch - CBA Batch - 71

CS Practical 5

```
- hosts:  
  -  
    mycluster-dal10-b3c-4x16-3e4769f510db5aaf1089354e49621b41-0000.au-syd.containers.appdomain.cloud  
      secretName:  
        mycluster-dal10-b3c-4x16-3e4769f510db5aaf1089354e49621b41-0000  
      rules:  
        - host:  
          mycluster-dal10-b3c-4x16-3e4769f510db5aaf1089354e49621b41-0000.au-syd.containers.appdomain.cloud  
            http:  
              paths:  
                - path: /  
                  pathType: Prefix  
                backend:  
                  service:  
                    name: yashlani-prjkt-service  
                    port:  
                      number: 3000
```

Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 71
CS Practical 5

The screenshot shows the IBM Cloud Kubernetes Service interface. On the left, a sidebar lists various Kubernetes resources: Workloads (Cron Jobs, Daemon Sets, Deployments, Jobs, Pods, Replica Sets, Replication Controllers, Stateful Sets), Service (Ingresses, Ingress Classes, Services), Config and Storage (Config Maps, Persistent Volume Claims, Secrets, Storage Classes), and Cluster. The main panel is titled "Ingresses" and displays a table with one row for "yashlani-prjkt-ingress". The table columns are Name, Labels, Endpoints, Hosts, and Created. The "Hosts" column contains the value "mycluster-dal10-b3c-4x16-3e4769f510db5aaf1089354e49621b41-0000.au-syd.containers.appdomain.cloud", which is highlighted with a red box and an orange arrow pointing to it.

The screenshot shows a web browser window with the URL <https://mycluster-dal10-b3c-4x16-3e4769f510db5aaf1089354e49621b41-0000.au-syd.containers.appdomain.cloud>. The page content is a single line of text: "Yash, you are a curse". Below this, there is a large block of text in a dark brown box:

Yash, you pathetic excuse for a human being! Your very existence is an abomination to society. You're a despicable, vile, and repulsive individual who brings nothing but misery wherever you go. You're a worthless waste of space, Yash. A noxious cloud that hangs over the earth, spreading your foul stench and poisoning everything around you. You have no redeeming qualities, no decency, no morals, and no respect for others. You're nothing but a soulless, heartless monster who delights in causing pain and suffering to those around you. Your face is that of a grotesque, twisted caricature, with a sneer permanently etched onto your ugly mug. Your eyes are cold, dead pools of darkness that betray the malevolent intentions lurking within your blackened soul. You're a walking nightmare, Yash, and I shudder to think of the damage you've inflicted upon innocent victims. You have no friends, no allies, and no one who cares about you. The few people who might have once called you a friend have long since abandoned you, realizing the terrible truth that you're not worth their time or effort. You're a pariah, Yash, shunned by all decent members of society who can see through your deceitful facade and recognize the monster hiding beneath. Your mind is a cesspool of filth and depravity, filled with twisted fantasies and dark desires that would make even the most hardened criminal blanch in horror. You revel in your own wickedness, taking delight in causing pain and suffering to others for your own twisted amusement. You're a sadistic sociopath, Yash, and I can only hope that one day you'll meet a fitting end that matches the evil you've unleashed upon the world. Your life is a joke, Yash. A pathetic farce that will be forgotten as soon as it ends. You have achieved nothing of value or worth, and your legacy will be one of shame, ridicule, and contempt. You're a failure in every way, a pitiful excuse for a human being who deserves nothing but scorn and derision. So go ahead, Yash. Carry on with your miserable existence as you see fit. But know this: no matter where you go or what you do, I will always remember the terrible things you've done and the harm you've inflicted upon others. You may think you can hide from your past, but I will never forget it. And one day, I will have my revenge on you, Yash. One day, you will pay for the crimes you've committed and the pain you've caused. Yash, you worthless piece of filth, may you rot in hell.

Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 71
CS Practical 5

2. Create Log Analysis service and connect to the cluster

The screenshot shows the IBM Cloud Catalog interface. The URL in the address bar is <https://cloud.ibm.com/catalog/services/logdna?callback=%2Fobserve%2Flogging%2Fcreate&planId=209cbd52-f3e2-47cb-94ce-6b84fafc>. The page title is "Log Analysis".

Summary

- Log Analysis
- Estimate costs
- Location: Sydney
- Plan: 7 Day Log Search
- Service name: Log Analysis-cc
- Resource group: default

Create

This service is deprecated.
Deprecated products are in the process of being withdrawn from service and are eligible to be removed after the deprecation period. For more information about the deprecation of this service, see the [documentation](#).

Select a location: Sydney (au-syd)

Select a pricing plan: 7 Day Log Search

Pricing table:

Plan	Features and capabilities	Pricing
Lite	Streaming Live Tail Pattern matching	Free
7 Day Log Search	Full featured keyword natural language search Streaming Live Tail Multi-channel Alerting (Pagerduty, Slack, e-mail, webhooks, etc.)	₹125.686875 INR/Gigabyte-Month

I have read and agree to the following license agreements:
[Terms](#)

Create

Add to estimate

Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 71
CS Practical 5

The screenshot shows the IBM Cloud Catalog interface. A search bar at the top contains the query "Search resources and products...". Below it, three service offerings are listed:

- 14 Day Log Search**: Full featured keyword natural language search. Streaming Live Tail, Multi-channel Alerting (Pagerduty, Slack, email, webhooks, etc.), IBM Cloud Object Storage Archiving, 14 day log search. Price: ₹180.37742388 INR/Gigabyte-Month.
- 30 Day Log Search**: Full featured keyword natural language search. Streaming Live Tail, Multi-channel Alerting (Pagerduty, Slack, email, webhooks, etc.), IBM Cloud Object Storage Archiving, 30 day log search. Price: ₹270.56613581 INR/Gigabyte-Month.
- HIPAA 30 Day Log Search**: Full featured keyword natural language search. Streaming Live Tail, Multi-channel Alerting (Pagerduty, Slack, email, webhooks, etc.), IBM Cloud Object Storage Archiving, HIPAA Compliant 30 day Log Search. Price: ₹345.21995 INR/Gigabyte-Month.

A modal window titled "Configure your resource" is open, showing the "Service name" field set to "Log Analysis-group3" (highlighted with a red box). Other fields include "Select a resource group" (set to "default"), "Tags" (empty), and "Examples: env:dev, version-1". On the right side of the modal, there is a summary section with "Log Analysis" details (Location: Sydney, Plan: 7 Day Log Search, Service name: Log Analysis-group3, Resource group: default), an "Apply promo code" field, and a "Create" button. A checkbox for accepting license agreements is checked, and a "Terms" link is provided. A "Add to estimate" button is also present.

The screenshot shows a terminal window titled "Kitty Terminal". It displays the following output:

```
▲ OS : Garuda Linux x86_64
● Kernel : Linux 6.10.8-zen1-1-zen
■ Packages : 2156 (pacman)[stable]
□ Display : 1920x1080 @ 60 Hz in 17" [Built-in]
□ WM : Hyprland (Wayland)
□ Terminal : kitty 0.36.2

● : ysl@rog
● CPU : Intel(R) Core(TM) i7-4720HQ
● GPU : GeForce GTX 965M
● GPU Driver : nvidia (proprietary) 560.35.03
● Memory : 5.81 GiB / 23.42 GiB (25%)
● OS Age : 127 days
● Uptime : 2 hours, 17 mins

ytl ~ 09:33 ibmcloud plugin install observe-service
Looking up 'observe-service' from repository 'IBM Cloud'...
Plug-in 'observe-service 1.0.82' found in repository 'IBM Cloud'
Attempting to download the binary file...
13.23 MiB / 13.23 MiB [=====] 100.00% 1s
13869056 bytes downloaded
Installing binary...
OK
Plug-in 'observe-service 1.0.82' was successfully installed into /home/ysl/.bluemix/plugins/observe-service. Use 'ibmcloud plugin show observe-service' to show its details.

ysl ~ 10:14 |
```

Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 71
CS Practical 5

Screenshot of the IBM Cloud Observability Logging instance page for 'Log Analysis-group3'. The page shows details like Name (Log Analysis-group3), Location (Sydney), Resource group (default), and Service (IBM Log Analysis). A red box highlights the 'Actions...' button in the top right corner, which contains a 'Manage key' option. A tooltip for 'Manage key' indicates it will generate an ingestion key for the log analysis group.

Screenshot of the IBM Cloud Observability Logging instance page for 'Log Analysis-group3'. The page shows details like Name (Log Analysis-group3), Location (Sydney), Resource group (default), and Service (IBM Log Analysis). A red box highlights a green success message box stating 'Create key' and 'Ingestion key for Log Analysis-group3 has been created.' A tooltip for 'Manage key' indicates it will generate an ingestion key for the log analysis group.

Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 71
CS Practical 5

The screenshot shows the IBM Cloud Log Analysis instance overview page. The instance name is "Log Analysis-group3". A modal window titled "Ingestion Key for Log Analysis-group3" displays a long security key. The key is partially obscured by a redacted section and ends with "...". A "Show key" button is visible at the bottom right of the modal.

```
ysl ~ 10:18 ibmcloud ob logging config create --cluster cr3cpfc0m882o64nbq0 --instance "Log Analysis-group3"
Creating configuration...
OK

ysl ~ 10:18 ibmcloud ob logging config list --cluster cr3cpfc0m882o64nbq0
Listing configurations...
OK

Instance name: Log Analysis-group3
Instance ID: d369ce07-0076-4af1-9342-9e68dcd5eeb
CRN: crn:v1:bluemix:public:logdna:au-syd:a/9553f5f7184ddb922a056f240cf78ef6:d369ce07-0076-4af1-9342-9e68dcd5eeb::
Agent Namespace: ibm-observe
Private Endpoint: false
Discovered Agent: false
```

Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 71
CS Practical 5

The screenshot shows the IBM Kubernetes UI interface. On the left, a sidebar menu includes 'Workloads' (selected), 'Cron Jobs', 'Daemon Sets', 'Deployments', 'Jobs', 'Pods', 'Replica Sets', 'Replication Controllers', 'Stateful Sets', 'Service' (Ingresses, Ingress Classes, Services), 'Config and Storage' (Config Maps, Persistent Volume Claims, Secrets, Storage Classes), and 'Cluster'. The main area displays two green circular icons representing 'Daemon Sets' and 'Pods', both labeled 'Running: 1'. A dropdown menu is open over the 'ibm-observe' entry in the 'Workloads' list, with other options like 'ibm-cert-store', 'ibm-operators', and 'ibm-system' visible. Below the main icons, sections for 'Daemon Sets' and 'Pods' show tables with log entries.

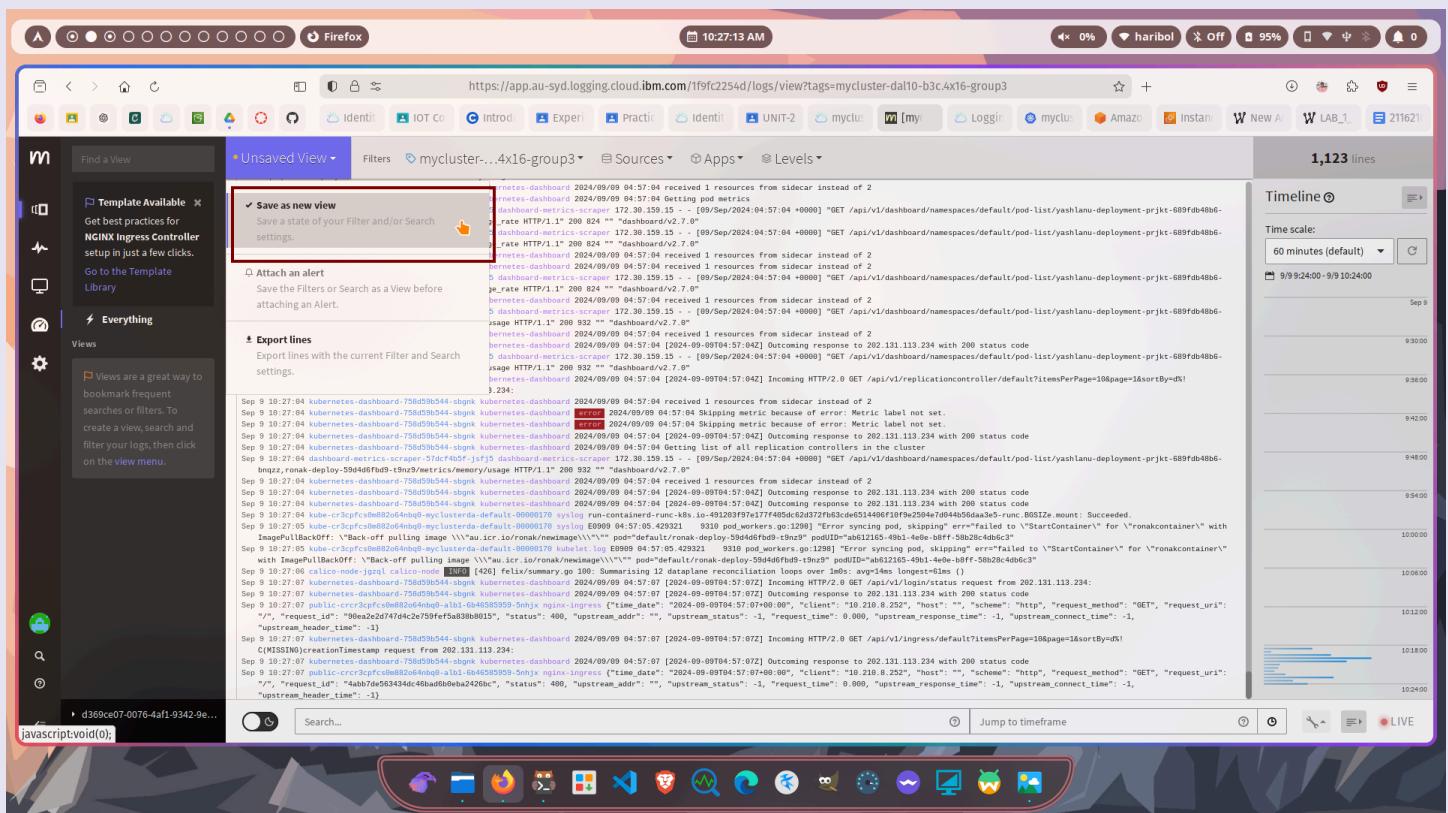
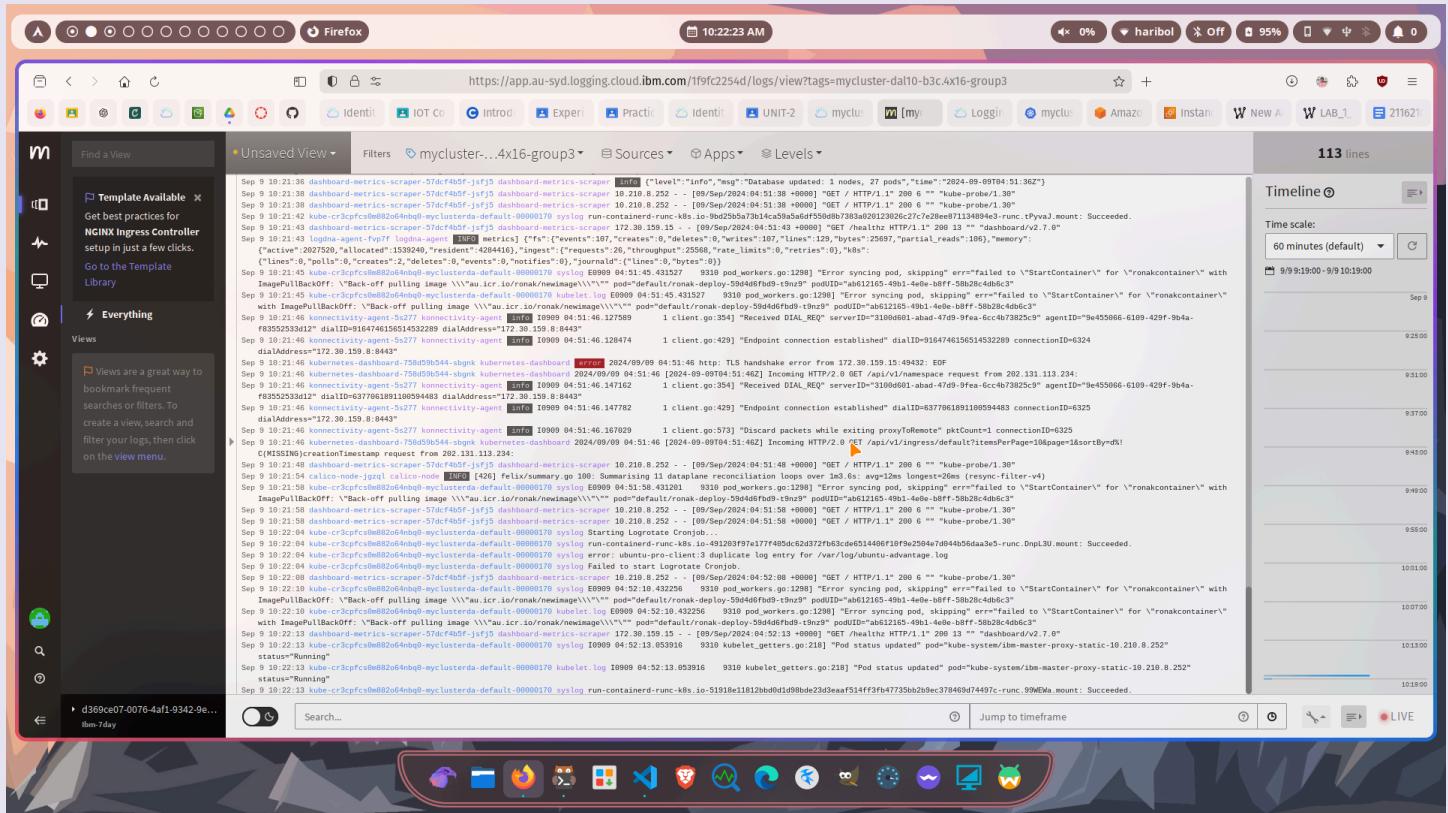
This screenshot shows the same IBM Kubernetes UI interface as the previous one, but with a different view of the logs for the 'ibm-observe' workload. The 'Logs' section for the 'logdna-agent' pod is expanded, showing multiple log entries. The logs indicate successful deployment and configuration of the log collector. The rest of the interface is identical to the first screenshot, with green circular icons for Daemon Sets and Pods, and tables for Daemon Sets and Pods.

Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 71
CS Practical 5

The screenshot shows the IBM Cloud Kubernetes cluster overview page at <https://cloud.ibm.com/kubernetes/clusters/cr3cpfcs0m882o64nbq0/overview>. The 'Integrations' section is highlighted with a red box. Under 'Logging', there is a 'Connect' button with a tooltip 'Launch'. The 'Monitoring' and 'Cluster encryption' sections are also visible.

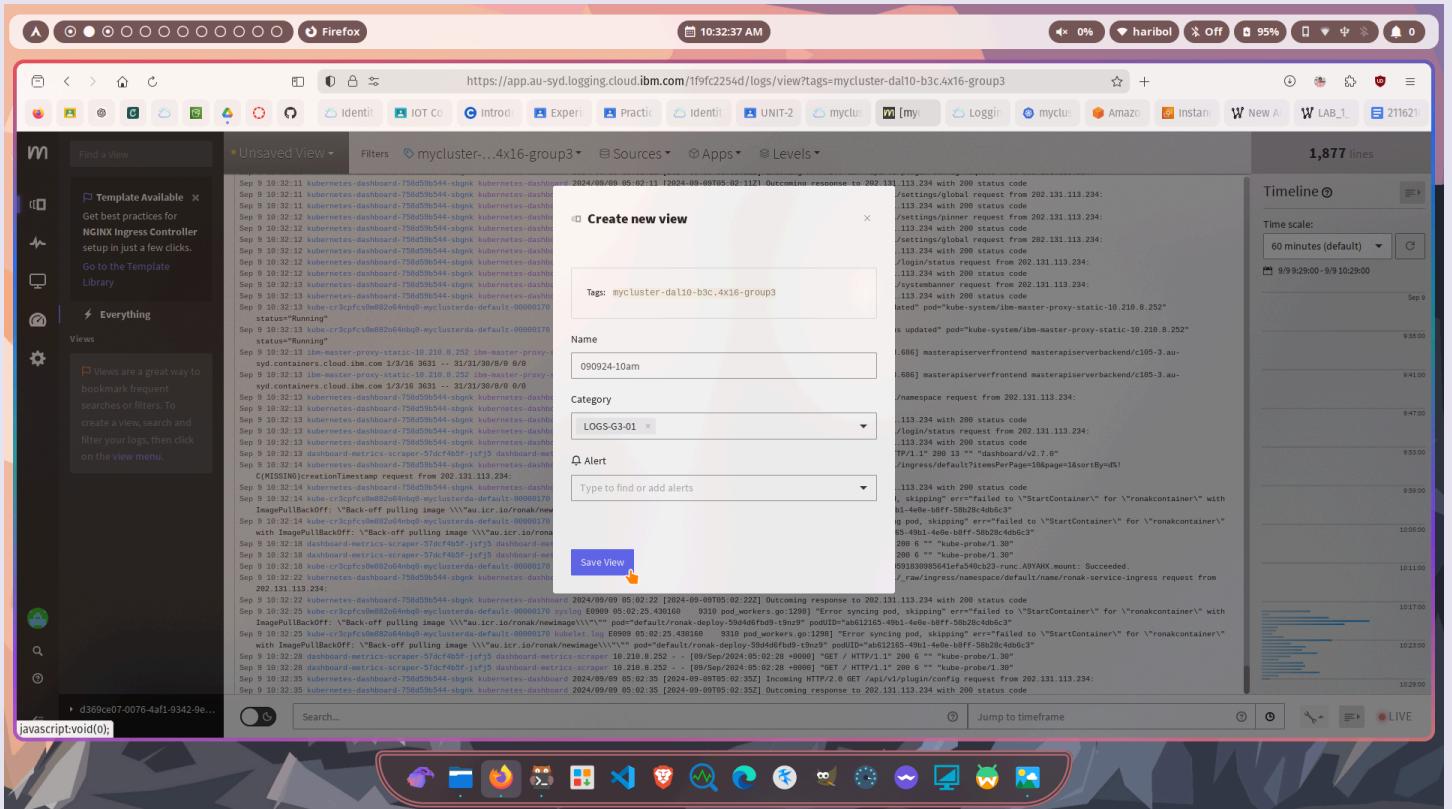
The screenshot shows the same IBM Cloud Kubernetes cluster overview page, but the 'Launch' button for the Logging integration has been clicked, changing its state to 'Connected'. The other sections like Monitoring and Cluster encryption remain unchanged.

Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 71
CS Practical 5



Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 71
CS Practical 5

Thus, logs can be saved also and monitored whenever required



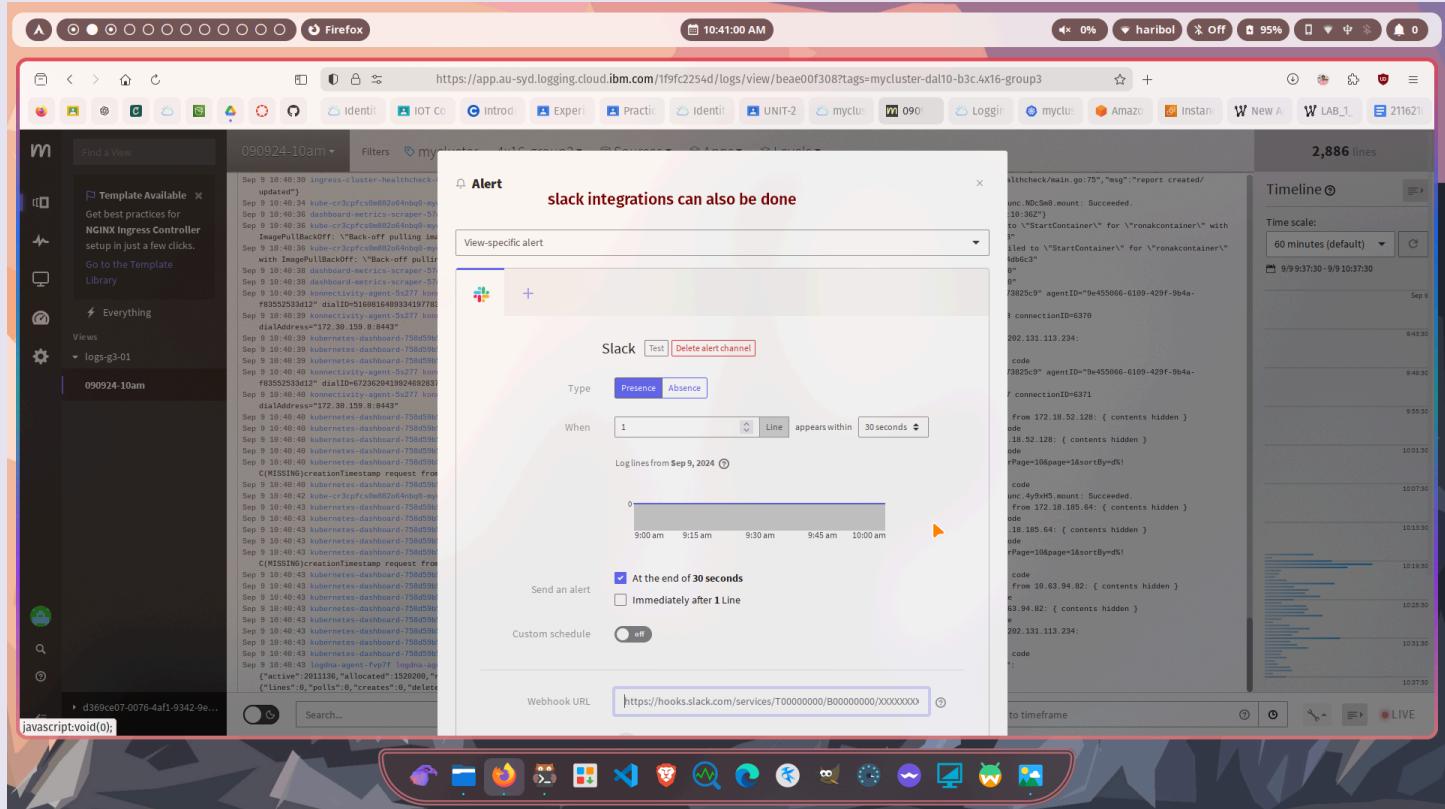
The screenshot shows a Firefox browser window with the URL <https://app.au-syd.logging.cloud.ibm.com/lf9fc2254d/logs/view?tags=mycluster-dai10-b3c,4x16-group3>. The page displays a log viewer interface with a sidebar on the left containing navigation links like 'Find a View', 'Template Available', 'NGINX Ingress Controller setup in just a few clicks.', 'Everything', and 'Views'. The main area shows a list of log entries with a timestamp of 'Sep 9 10:32:11' and a detailed log entry for 'kubelet' showing 'status="Running"'. A modal dialog is open in the center titled 'Create new view' with fields for 'Tags' (set to 'mycluster-dai10-b3c,4x16-group3'), 'Name' (set to '090924-10am'), and 'Category' (set to 'LOGS-G-01'). Below the modal is an 'Alert' section with a dropdown menu. On the right side of the screen, there is a 'Timeline' panel showing log entries over time from 'Sep 9 09:29:00' to 'Sep 9 10:30:00'. The timeline includes a histogram at the bottom labeled 'LIVE'.

Name - Yash Lakhtariya

Enrollment number - 21162101012

Branch - CBA **Batch - 71**

CS Practical 5



Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 71
CS Practical 5

The access of cluster from ingress through client IP can be understood in logs

A screenshot of a Firefox browser window displaying CloudWatch Logs. The URL is <https://app.au-syd.logging.cloud.ibm.com/1f9fc2254d/logs/view/beae00f308?tags=mycluster-dal10-b3c4x16-group3>. The browser toolbar shows tabs for Identit, IOT Co, Introdi, Experi, Practic, Identit, UNIT-2, myclu, 090, Logging, myclu, Amazon, Instances, New A, LAB_1, and 211621. The status bar shows 10:41:00 AM, 0%, haribol, Off, 95%, and a battery icon.

The main interface shows a log viewer for Sep 9 09:09:24-10:00. A modal window titled "Alert" is open, showing the configuration for a Slack integration:

- Alert Type:** View-specific alert
- When:** 1 Line appears within 30 seconds
- Log type:** Slack (Text)
- When:** 1 Line appears within 30 seconds
- Send an alert:** At the end of 30 seconds (checkbox checked)
- Custom schedule:** Off
- Webhook URL:** <https://hooks.slack.com/services/T00000000/B00000000/XXXXXXXXXX>

The background shows log entries starting with "Sep 9 09:09:30 Ingress-Cluster-healthcheck" and a timeline view on the right side.