

NAME: KSHITIJ GUPTA

Enrolment Number: 21162101007

Sub: CS

Practical – 5[Batch-71]

task is to learn how to add and configure the Ingress component in Kubernetes

The screenshot shows the IBM Cloud Kubernetes dashboard for a cluster named `mycluster-syd01-u3c.2x4-group2`. The `Ingress` tab is selected. An overall warning message is displayed: "Some Ingress components are in a warning state. To view the state of your Ingress components, run `ibmcloud ks ingress status-report get`." Below this, a table lists the status of various ingress components:

Component	Status	Status message
ingress-controller-configmap	Healthy	--
alb-healthcheck-ingress	Healthy	--
public-crrc3cp7vs0jfn8bg998g-alb1	Warning	One or more ALB pod is not in running state (ERRADRUH). Docs
mycluster-syd01-u3-325769-3e4769f510db5aaf1089354e49621b41-0000.au-syd.containers.appdomain.cloud	Healthy	--
ibm-cert-store/mycluster-syd01-u3-325769-3e4769f510db5aaf1089354e49621b41-0000	Healthy	--
kube-system/mycluster-syd01-u3-325769-3e4769f510db5aaf1089354e49621b41-0000	Healthy	--
default/mycluster-syd01-u3-325769-3e4769f510db5aaf1089354e49621b41-0000	Healthy	--

Step-1: go to cluster and check ingress part

The screenshot shows the IBM Cloud Kubernetes dashboard. The left sidebar has sections for Clusters, Overview, Worker nodes, Worker pools, Ingress (selected), DevOps, and Help. The main area is titled "mycluster-syd01-u3c.2x4-group2". Under the "Ingress" section, the "Domains" tab is selected. A table lists one domain entry:

Domain	Records	Status
mycluster-syd01-u3-325769-3e4769f510db5aaf1089354e49621b41-0000.au-syd.containers.appdomain.cloud (Default)	159.23.71.178	OK

At the bottom, there are buttons for "Create" and "Actions...". The status bar at the bottom right shows "08:38 09-09-2024".

Lunch the kubernets and copy the secret

The screenshot shows the Kubernetes UI. The left sidebar has sections for Workloads, Config And Storage, and Service (selected). The main area shows a secret named "mycluster-syd01-u3-325769-3e4769f510db5aaf1089354e49621b41-0000". The "Data" section contains two files:

Name	Content
tls.crt	3973 bytes
tls.key	1679 bytes

The status bar at the bottom right shows "08:40 09-09-2024".

In ingress set your ingress

```
apiVersion: networking.k8s.io/v1
kind: Ingress
metadata:
  name: kshitij
  annotations:
    kubernetes.io/tls-acme: "true"
spec:
  tls:
  - hosts:
    - app.mydomain.com
    secretName: mycluster-syd01-u3-325769-3e4769f510db5aaf1089354e49621b41-0000
  rules:
  - host: >-
    mycluster-syd01-u3-325769-3e4769f510db5aaf1089354e49621b41-0000.au-syd.containers.appdomain.cloud
    http:
      paths:
      - path: /
        pathType: Prefix
        backend:
          service:
            name: kshitij-service
            port:
              number: 8000
      status:
      loadBalancer:
        ingress:
        - ip: 159.23.71.178
```

This action is equivalent to: `kubectl apply -f spec.yaml`

And lunch your ingress

Hello docker is running

Code for ingress:

kind: Ingress

apiVersion: networking.k8s.io/v1

metadata:

name: guptagnu-service-ingress

namespace: default

uid: 6e7e7706-07b9-46dd-a180-17bfc93b9676

resourceVersion: '1863984'

generation: 1

creationTimestamp: '2024-09-09T04:05:08Z'

annotations:

nginx.ingress.kubernetes.io/from-to-www-redirect: 'true'

nginx.ingress.kubernetes.io/rewrite-target: /

nginx.ingress.kubernetes.io/ssl-redirect: 'true'

managedFields:

- manager: dashboard

operation: Update

apiVersion: networking.k8s.io/v1

time: '2024-09-09T04:05:08Z'

fieldsType: FieldsV1

fieldsV1:

f:metadata:

f:annotations:

..: {}

f:nginx.ingress.kubernetes.io/from-to-www-redirect: {}

f:nginx.ingress.kubernetes.io/rewrite-target: {}

```
f:nginx.ingress.kubernetes.io/ssl-redirect: {}

f:spec:
  f:ingressClassName: {}
  f:rules: {}
  f:tls: {}

- manager: nginx-ingress-controller
  operation: Update
  apiVersion: networking.k8s.io/v1
  time: '2024-09-09T04:05:32Z'
  fieldsType: FieldsV1
  fieldsV1:
    f:status:
      f:loadBalancer:
        f:ingress: {}
    subresource: status

spec:
  ingressClassName: public-iks-k8s-nginx
  tls:
    - hosts:
        - >-
          mycluster-syd01-u3-325769-3e4769f510db5aaf1089354e49621b41-0000.au-
          syd.containers.appdomain.cloud
        secretName: mycluster-syd01-u3-325769-3e4769f510db5aaf1089354e49621b41-
        0000
  rules:
    - host: >-
      mycluster-syd01-u3-325769-3e4769f510db5aaf1089354e49621b41-0000.au-
      syd.containers.appdomain.cloud
```

http:

paths:

- **path:** /

pathType: Prefix

backend:

service:

name: kshitij-service

port:

number: 8000

status:

loadBalancer:

ingress:

- **ip:** 159.23.71.178

Part-2:

Create Log Analysis Service:

The screenshot shows the IBM Cloud Catalog interface. A prominent message at the top left states: "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](#)." To the right, a summary panel displays details for a "Log Analysis" service instance.

Summary

Log Analysis [Estimate costs](#)

Location: Sydney
Plan: 7 Day Log Search
Service name: Log Analysis-kshitij
Resource group: default

Apply promo code

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

Create

Add to estimate

Log Analysis

Log collection and search for IBM Cloud. Define alerts and design custom views to monitor application and system logs.

Create [About](#)

Type: Service
Provider: IBM

Last updated: 07/01/2024

Category: Logging and monitoring

Compliance: EU Supported, IAM-enabled

Location: Sydney, São Paulo, Toronto, Frankfurt, Madrid, London, Chennai, Osaka, Tokyo, Washington DC, Dallas

Select a location: Sydney (au-syd)

Select a pricing plan: 7 Day Log Search

Displayed prices do not include tax. Monthly prices shown are for country or location: India

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, email, webhooks, etc.) IBM Cloud Object Storage Archiving 14 day log search	₹125.686875 INR/Gigabyte-Month

Configure your resource

Service name: Log Analysis-kshitij

Select a resource group: default

Tags: env:dev, version:1

Examples: env:dev, version:1

System status bar: 27°C Mostly cloudy, ENG, 09:55, 09-09-2024

The screenshot shows the IBM Cloud Observability interface. On the left, a sidebar lists 'Observability' and 'Logging Instances'. The main area displays 'Logging instances' with two entries:

Name	Status	Resource group	Region	Plan	View
Log Analysis-CB	Active	default	Sydney	Lite <small>Expires in 30 days</small>	Open dashboard
Log Analysis-kshitij	Active	default	Sydney	7 Day Log Search	Open dashboard

At the bottom, there are pagination controls: 'Items per page: 25', '1–2 of 2 items', and '1 of 1 page'.

The screenshot shows the details page for the 'Log Analysis-kshitij' instance. The top navigation bar includes 'Observability / Logging instances / Log Analysis-kshitij' and 'Actions...'. The main content is divided into sections:

- Overview**: Shows 'Logging sources'.
- Details**: Includes fields for 'Name' (Log Analysis-kshitij), 'Location' (Sydney), 'Resource group' (default), and 'Service' (IBM Log Analysis). A 'Configure platform logs' button is highlighted with a blue border.
- Plan**: Shows 'Pricing plan' (7 Day Log Search) and an 'Edit' button.
- Getting started with logging**: Contains a 'Get started' button.

At the bottom, there are standard Windows taskbar icons and system status indicators.

Open dashboard and explore the other services:

The screenshot shows the IBM Cloud Observability Log Analysis interface. The left sidebar includes sections for Views, Alerts, Archiving, Streaming, Billing, Parsing, and Support. The main area displays a search bar with the query "Everything" and a timeline section showing "0 lines". A message box indicates "No data found." Below the search bar, there's a "Find views" dropdown and a "Search..." input field. The bottom navigation bar includes icons for Home, Log Analysis, Catalog, Manage, and Help.

The screenshot shows the "Manage Categories" page within the IBM Cloud Observability Log Analysis interface. The left sidebar remains the same. The main area features a "Views" dropdown menu and a search bar with the placeholder "Find views". On the right, there are two panels: "All Views" (empty) and "Categories" (also empty). A "Drag & Drop" arrow points from the "All Views" panel to the "Categories" panel. The bottom navigation bar is identical to the previous screenshot.

The screenshot shows the IBM Cloud Kubernetes cluster overview page. At the top, there are sections for 'Ingress secrets instance' (None) and 'Ingress ALB automatic updates' (Enabled). Below this is the 'Integrations' section with tabs for 'Logging' (Connect), 'Monitoring' (Connect), and 'Cluster encryption' (Enable). The 'Add-ons' section lists several options available to install, including 'Managed Istio' (Install, Docs), 'Static Route' (Install, Docs), and 'Diagnostics and Debug Tool' (Install, Docs). The 'ALB OAuth Proxy' is also mentioned. The bottom of the screen shows a Windows taskbar with various pinned icons and a system tray indicating 'Nifty midcap -0.67%'.

In Log Analysis create the Key and use that key into cluster area to logging or connect with cluster

The screenshot shows the IBM Cloud Log Analysis instance details page for 'Log Analysis-group2'. It includes sections for 'Overview', 'Details' (showing Name: Log Analysis-group2, Location: Sydney, Resource group: default, Service: IBM Log Analysis), and 'Plan' (Pricing plan: 7 Day Log Search). A sidebar on the right provides actions like 'Open dashboard', 'Manage key' (which is highlighted), 'View docs', 'Access report', 'Manage access', 'Undocked dashboard...', and 'Delete'. The bottom of the screen shows a Windows taskbar with various pinned icons and a system tray indicating 'Nifty smicap -1.24%'.

cloud.ibm.com/observability/logging/46bc513c-d75f-4ffc-8868-05f1d0d02a66/overview

IBM Cloud Search resources and products... Catalog Manage 2716063 - IBM India Pvt Ltd, C/o S...

Deprecated: Log Analysis
IBM Log Analysis will be discontinued on 30 March 2025 and replaced by IBM Cloud Logs. A migration tool is available to assist with a migration to IBM Cloud Logs. Learn more

Observability / Logging instances / Log Analysis-group2 Active Add tags

Open dashboard Actions...

Overview Details

Name Log Analysis-group2

Ingestion Key for Log Analysis-group2

The ingestion key is a security key that you use to configure agents and successfully forward events to your IBM Log Analysis instance in IBM Cloud. Learn more

View ingestion key 4d8a93e6b7eb94d2b71c21448ca8001c Hide key

Created 9/9/2024, 9:56 AM

CRN crn:v1:bluemix:pl

Plan

Pricing plan 7 Day Log Search

Getting started with logging

Type here to search 27°C Mostly cloudy 1006 09-09-2024

cloud.ibm.com/kubernetes/clusters/cr3cp7vs0jfnd8bg998g/overview

IBM Cloud Search resources and products... Catalog Manage 2716063 - IBM India Pvt Ltd, C/o S...

Networking

Service endpoint URL

Public enabled Copy link ⓘ Private disabled Copy link ⓘ

Ingress subdomain mycluster-syd01-u3-325769-3e4769f510db5aaaf1089354e49621b41-0000.au-syd.contain...

Ingress secrets instance None

Manage

Ingress ALB automatic updates Enabled

Integrations

Logging Connect Monitoring Connect Cluster encryption Enable

Add-ons

Enhance your cluster's capabilities by installing add-ons. Learn more about add-ons in our docs.

Available to install

Managed Istio Simplify traffic, policy, and telemetry management across the microservices that run in your cluster.

Install Docs

Diagnostics and Debug Tool Test and gather information about various components in your cluster to help debug issues.

Install Docs

Static Route Add static routing rules to your worker nodes to manage routing between your cluster and other networks

ALB OAuth Proxy Integrate IBM Cloud App ID with your Ingress ALBs to enforce app authentication. See the docs for information about using the OAuth Proxy with APIs that run the Kubernetes Ingress controller.

Type here to search BSE smlcap -1.13% 10:08 09-09-2024

Networking

Service endpoint URL

- Public enabled Copy link
- Private disabled Copy link

Ingress secrets instance
None

Ingress subdomain
mycluster-syd01-u-3-325769-3e4769f510db5aaf1089354e49621b41-0000.au-syd.ctl

Ingress ALB automatic updates Enabled

Integrations

Logging

Monitoring

Cluster encryption

Add-ons

Enhance your cluster's capabilities by installing add-ons. Learn more about add-ons in our [docs](#).

Available to install

Managed Istio Simplify traffic, policy, and telemetry management across the microservices that run in your cluster. <input type="button" value="Install"/> <input type="button" value="Docs"/>	Diagnostics and Debug Tool Test and gather information about various components in your cluster to help debug issues. <input type="button" value="Install"/> <input type="button" value="Docs"/>
Static Route Add static routing rules to your worker nodes to manage routing between your cluster and other networks <input type="button" value="Install"/> <input type="button" value="Docs"/>	ALB OAuth Proxy Integrate IBM Cloud App ID with your Ingress ALBs to enforce app authentication. See the docs for information about using the OAuth Proxy with ALBs that run the Kubernetes Ingress controller. 27°C Mostly cloudy ENG 09-09-2024

Explore the CLI Services

Login into CLI

```

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS COMMENTS
User: kshitijgupta21@gnu.ac.in
Account: IBM India Pvt Ltd, C/o Software (9553f5f7184dd922a056f240cf78ef6) <-> 2716063
Resource group: No resource group targeted, use 'C:\Program Files\IBM\Cloud\bin\ibmcloud.exe target -g RESOURCE_GROUP'
PS D:\SEM-7\CS\PR5> * History restored

Warning: PowerShell detected that you might be using a screen reader and has disabled PSReadLine for compatibility purposes. If you want to re-enable it, run 'Import-Module PSReadLine'.

PS D:\SEM-7\CS\PR5> 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...
13.38 MiB / 13.38 MiB [=====] 100.00% 1s
14024704 bytes downloaded
Installing binary...
OK
Plug-in 'observe-service 1.0.82' was successfully installed into C:\Users\Kshitij\.bluemix\plugins\observe-service. Use 'C:\Program F
iles\IBM\Cloud\bin\ibmcloud.exe plugin show observe-service' to show its details.
PS D:\SEM-7\CS\PR5>

```

`ibmcloud ob logging config create --cluster <clusterID/NM> --instance <LogDNA ID/NM>`

```

+ FullyQualifiedErrorId : CommandNotFoundException
PS D:\SEM-7\CS\PR5> ibmcloud ob logging config create --cluster cr3cp7vs0jfn8bg998g --instance "Log Analysis-group2"
Creating configuration...
FAILED
A logging or monitoring configuration for this cluster already exists. To use a different configuration, delete the existing configuration and try again. (S0013)

Incident ID: dc7e7cba-b4c7-4c06-8098-40ac4ade7ae4,dc7e7cba-b4c7-4c06-8098-40ac4ade7ae4

PS D:\SEM-7\CS\PR5>

```

Verify that the logging configuration was added to your cluster using the following

Command: ibmcloud ob logging config list --cluster <cluster-name-or-ID>

```
PS D:\SEM-7\CS\PR5> ibmcloud ob logging config list --cluster ^V
Listing configurations...

PS D:\SEM-7\CS\PR5> ibmcloud ob logging config list --cluster cr3cp7vs0jfnd8bg998g
Listing configurations...

OK

Instance name: Log Analysis-group2
Instance ID: 46bc513c-d75f-4ffc-8868-05f1d0d02a66
CRN: crn:v1:bluemix:public:logdna:au-syd:a/9553f5f7184ddb922a056f240cf78ef6:46bc513c-d75f-4ffc-8868-05f1d0d02a66:
Agent Namespace: ibm-observe
Private Endpoint: false
Discovered Agent: false
PS D:\SEM-7\CS\PR5>
```


The screenshot shows the IBM Cloud Kubernetes Service (Kubernetes) dashboard. On the left, there is a sidebar with navigation links for Cron Jobs, Daemon Sets, Deployments, Jobs, Pods, Replica Sets, Replication Controllers, Stateful Sets, and Services. Under Services, there are Ingresses (3) and Services (1). Below the sidebar, there is a section titled "Config and Storage" with links for Config Maps (1), Persistent Volume Claims (1), Secrets (1), and Storage Classes. At the bottom of the sidebar, there is a "Cluster" section with a dropdown menu set to "mycluster".

The main content area has a title "Workloads". It features three pie charts under "Workload Status":

- Deployments: Pending: 1 (yellow), Running: 2 (green), Failed: 3 (red). Total: 3.333%.
- Pods: Pending: 1 (yellow), Running: 2 (green), Failed: 3 (red). Total: 3.
- Replica Sets: Pending: 1 (yellow), Running: 7 (green), Failed: 3 (red). Total: 7.

Deployments

Name	Images	Labels	Pods	Created
gnu-deploy-testing	Show all	-	0 / 1	3.days.ago
raj-deploy1	Show all	-	1 / 1	3.days.ago

Select the ibm-observe namespace from the drop-down

The screenshot shows the Kubernetes Workloads interface. On the left, there's a sidebar with various resource types like Cron Jobs, Daemon Sets, Deployments, etc. A dropdown menu is open over the 'Workloads' button, showing options: 'All namespaces', 'NAMESPACES', 'calico-system', and 'default'. The main area displays two large green circles representing 'Daemon Sets' and 'Pods', both labeled 'Running: 1'. Below these are tables for 'Daemon Sets' and 'Pods'. The 'Daemon Sets' table has one row for 'logdna-agent'. The 'Pods' table is currently empty. At the bottom, there's a search bar and a taskbar with icons for various applications.

Go to the Kubernetes cluster instance and scroll to Launch

The screenshot shows the IBM Cloud Kubernetes cluster overview page. It includes sections for 'Worker node health' (1 total worker nodes, all normal), 'Networking' (service endpoint URL set to 'Public enabled'), 'Integrations' (logging, monitoring, cluster encryption), and 'Add-ons' (Managed Istio). The interface is clean with a light color scheme and standard UI elements like buttons and dropdowns. A taskbar at the bottom includes icons for file operations and system status.

You can see all the pod logs in the cluster

The screenshot shows a browser window with several tabs open, each displaying log entries from different Kubernetes clusters and namespaces. The tabs include:

- Practical
- Logging
- Practical
- Document
- myclust...
- [myclust...]
- myclust...
- myclust...
- 503 Serv...
- 503 Serv...
- 503 Serv...

The main content area displays a log entry from the 'mycluster-sy01-u3c-2x4-group2' namespace. The log entry is timestamped at Sep 9 10:25:49 and contains details about a pod named 'rajapp3'. The log message indicates that the pod is restarting failed container 'rajapp3' due to a deployment error. The log ends with the message 'Error syncing pod, skipping'.

On the right side of the interface, there is a 'Timeline' panel showing a timeline of events from Sep 9 9:23:00 to Sep 9 10:23:00. The timeline shows various log entries and events, with a count of 4,210 lines.

Save the view and set the notification of each information :

The screenshot shows a 'Create new view' dialog box overlaid on a log viewer interface. The dialog box has the following fields:

- Tags:** mycluster-sy01-u3c-2x4-group2
- Name:** My View
- Category:** Type to find or add categories
- Alert:** Type to find or add alerts

The background log viewer interface shows log entries from the 'mycluster-sy01-u3c-2x4-group2' namespace. One specific log entry is highlighted, showing a deployment error for a pod named 'rajapp3'. The log message indicates that the pod is restarting failed container 'rajapp3' due to a deployment error. The log ends with the message 'Error syncing pod, skipping'.

On the right side of the interface, there is a 'Timeline' panel showing a timeline of events from Sep 9 10:28:11 to Sep 9 10:28:41. The timeline shows various log entries and events, with a count of 140 lines.

Practical | IBM Cloud | Practical | Document | myclust... | hello » | myclust... | myclust... | 503 Serv... | 503 Serv... | +

app.au-syd.logging.cloud.ibm.com/4d8a93e6b7/logs/view?q=hello

Create new view

Query: hello

Name: kshitij

Category: Type to find or add categories

Alert: View-specific alert

Email Test Delete alert channel

Type: Presence Absence

When: 1 Line appears within 30 seconds

Log lines... Loading log lines...

Timeline 0 lines

Time scale: 30 seconds

9/9 10:35:35 - 9/9 10:36:05

No data found.

Type here to search

File Home Search Logins Alert Chat

IBM 27°C Mostly cloudy 10:39 09-09-2024

Practical | IBM Cloud | Practical | Document | myclust... | hello » | myclust... | myclust... | 503 Serv... | 503 Serv... | +

app.au-syd.logging.cloud.ibm.com/4d8a93e6b7/logs/view?q=hello

Create new view

Email Test Delete alert channel

Type: Presence Absence

When: 1 Line appears within 30 seconds

Log lines from Sep 9, 2024

0 9:00 am 9:15 am 9:30 am 9:45 am 10:00 am

Send an alert At the end of 30 seconds Immediately after 1 Line

Custom schedule off

Recipients: kshitijpgupta21@gnu.ac.in

Timezone: (GMT -10:00) Pacific/Johnston

Save View

Timeline 0 lines

Time scale: 30 seconds

9/9 10:36:47 - 9/9 10:37:17

No data found.

Type here to search

File Home Search Logins Alert Chat

IBM 27°C Mostly cloudy 10:39 09-09-2024

Screenshot of update:

The screenshot shows a Gmail inbox with 905 messages. A specific email from 'Mezmo Alerts <alerts@mezmo.com>' is selected, titled 'kshitij - 1 matched line'. The message body contains the text 'kshitij 🎉' and '1 matched line'. Below the message is a code snippet:

```
Sep 08 22:35:24 public-crccr3cp7vs0jfn8bg998g-alb1-75b57df475-xpmj nginx-ingress {"time_date": "2024-09-09T09:35:24+00:00", "client": "172.30.150.116", "host": "159.23.71.178:88", "scheme": "http", "request_method": "POST", "request_uri": "/hello.world", "request_id": "ab8ef38d2b140c1c9196a34d5498b4ec", "status": 404, "upstream_addr": "", "upstream_status": -1, "request_time": 0.000, "upstream_response_time": -1, "upstream_connect_time": -1, "upstream_header_time": -1}
```

Below the message, there are links to mute the alerts for 1 Hour, 6 Hours, 12 Hours, or 1 Day. The Gmail interface includes a sidebar with Mail, Chat, Meet, and Labels sections, and a bottom taskbar with various icons.

Agent Key:

The screenshot shows the Kubernetes Secrets page for the 'ibm-observe' namespace. The left sidebar lists various cluster resources: Jobs, Pods, Replica Sets, Replication Controllers, Stateful Sets, Service, Ingresses, Ingress Classes, Services, Config and Storage, Config Maps, Persistent Volume Claims, Secrets (which is selected), and Storage Classes. The main content area displays a table of secrets:

Name	Labels	Type	Created
logdna-agent-key	-	Opaque	35 minutes ago

The bottom of the screen shows a Windows taskbar with various pinned icons and system status information.

Important Command:

download the Kubernetes configuration files-

ibmcloud ks cluster config --cluster <Cluster ID>

Remove the secret from your Kubernetes cluster.

kubectl delete secret logdna-agent-key -n ibm-observe

Remove the logging agent on every worker(node) of your Kubernetes cluster.

kubectl delete secret logdna-agent-key -n ibm-observe

kubectl delete daemonset logdna-agent -n ibm-observe

Verifying the same by listing the pods of that namespace

Kubectl get pods -n ibm-observe

Verify that the logging configuration was been deleted using the following command:

ibmcloud ob logging config list --cluster <cluster_id>