

Name: Yash Lakhtariya

En no: 21162101012

Class: 7A (CBA) Batch - 7I

Sub: Cloud Security Assignment - 1

[a - 1]

[CIA triad]

- C stands for Confidentiality, which means to limit access to data using rules
- I stands for Integrity, which is the assurance that data is accurate, trustworthy
- A stands for Availability, which stands for guarantee of reliable access to the data by authorized entities
- In context of cloud, all these are to be taken care by provider & consumer

⇒ Measures to ensure cloud security :

(WQ(i)) Confidentiality : The goal is to ensure

- As multiple users are utilizing cloud services & resources, they must remain isolated with each other by providers
 - Only authorized users should be able to access data, implement using Authentication, Authorization through IAM, Roles, Users, Groups
 - Also external tools like Key Protect, Security Benchmarks of CIS can be used to ensure Confidentiality.
- ### (ii) Integrity :

- Integrity can be ensured using hashing algorithms like MAC (Message Authentication Code), Merkle Tree, etc.
- PDP (Provable Data Possession), and POF

(Proof of Possession) ensures that the data is safe with server and client owns it, along with Proof of Ownership (Power)

(iii) Availability: even algorithm of

proper functioning of services.
→ It can be ensured by protection from DOS (Denial of Service) Attacks which disturb availability of services.

→ Continuous monitoring and using CIS Benchmarks ensure availability is not disturbed by attackers / hackers.

Also, proper data replication, distribution and disaster recovery are responsible measures for both provider and consumer.

: Chapter 11

⇒ This way, following some steps or using external / inbuilt security services ensure CIA triad measures for cloud security.

909 (part 1) (part 2) 909

2020-09-22 Q-2 Jyoti 207 ←
Topic: Object Storage

⇒ The steps to do so on a IBM Cloud Object Storage service with some data in a bucket suppose, are:

→ For authorization, set IAM Access of Policies (as required) 29/9/2020 transit

→ Also for operation specific access, the roles for bucket are: Object Reader, Object Writer, Reader, Writer and Manager in Roles section of service.

→ For encryption, enable settings for Encryption at Rest and at Transit so IBM cloud provides AES 256 encryption for data in buckets.

→ In Monitoring section, enable 'Access Logs' option

→ Change 'Lifecycle Policy' to 90 days for moving ~~data~~ unused data at different location

→ For internal-only access, there are different ways:

(i) ~~no or no idea about it~~
~~use Firewalls and company's Network & IP only rules in tit and a pi~~

(ii) Create VPC endpoint for S3 bucket and use VPC Gateway Endpoints rules to restrict access.

~~use VPC endpoint for S3 bucket and use VPC Gateway Endpoints rules to restrict access~~
~~use VPC endpoint for S3 bucket and use VPC Gateway Endpoints rules to restrict access~~

~~use VPC endpoint for S3 bucket and use VPC Gateway Endpoints rules to restrict access~~
~~use VPC endpoint for S3 bucket and use VPC Gateway Endpoints rules to restrict access~~

~~use VPC endpoint for S3 bucket and use VPC Gateway Endpoints rules to restrict access~~

~~use VPC endpoint for S3 bucket and use VPC Gateway Endpoints rules to restrict access~~

Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 71
CS Assignment 1

1. Create Activity tracker service

The screenshot shows the IBM Cloud Catalog interface. A modal window is open for creating a new service instance. The service selected is 'Cloud Activity Tracker' located in Madrid, with the 'Plan: Lite' option selected. The service name is set to 'Claaud-Ektiwiti-Trekkr-ysl'. The configuration section shows the service name 'Claaud-Ektiwiti-Trekkr-ysl' and the resource group 'default' selected. A note indicates that only one Lite plan instance can be created per resource group. The 'Create' button is visible at the bottom right of the modal.

Cloud Activity Tracker - IBM Cloud Catalog

Cloud Activity Tracker
Location: Madrid
Plan: Lite

Service name: Claaud-Ektiwiti-Trekkr-ysl
Resource group: default

Existing Lite plan instance
You can have only 1 Lite plan instance of this service per resource group. [Delete](#) your current Lite plan instance in default resource group to create a new one, or [view the existing instance](#).

Configure your resource

Service name: Claaud-Ektiwiti-Trekkr-ysl

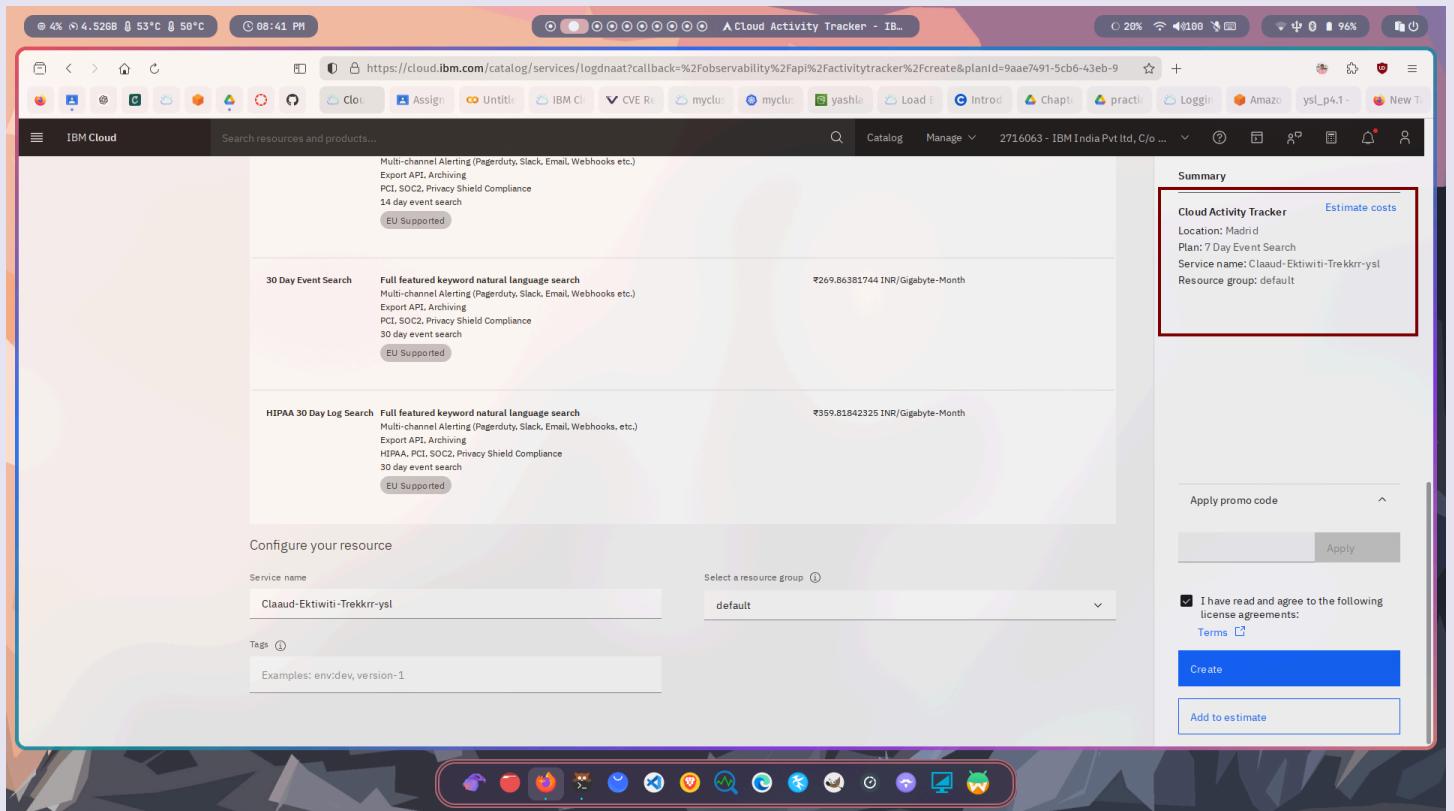
Select a resource group: default

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 Assignment 1



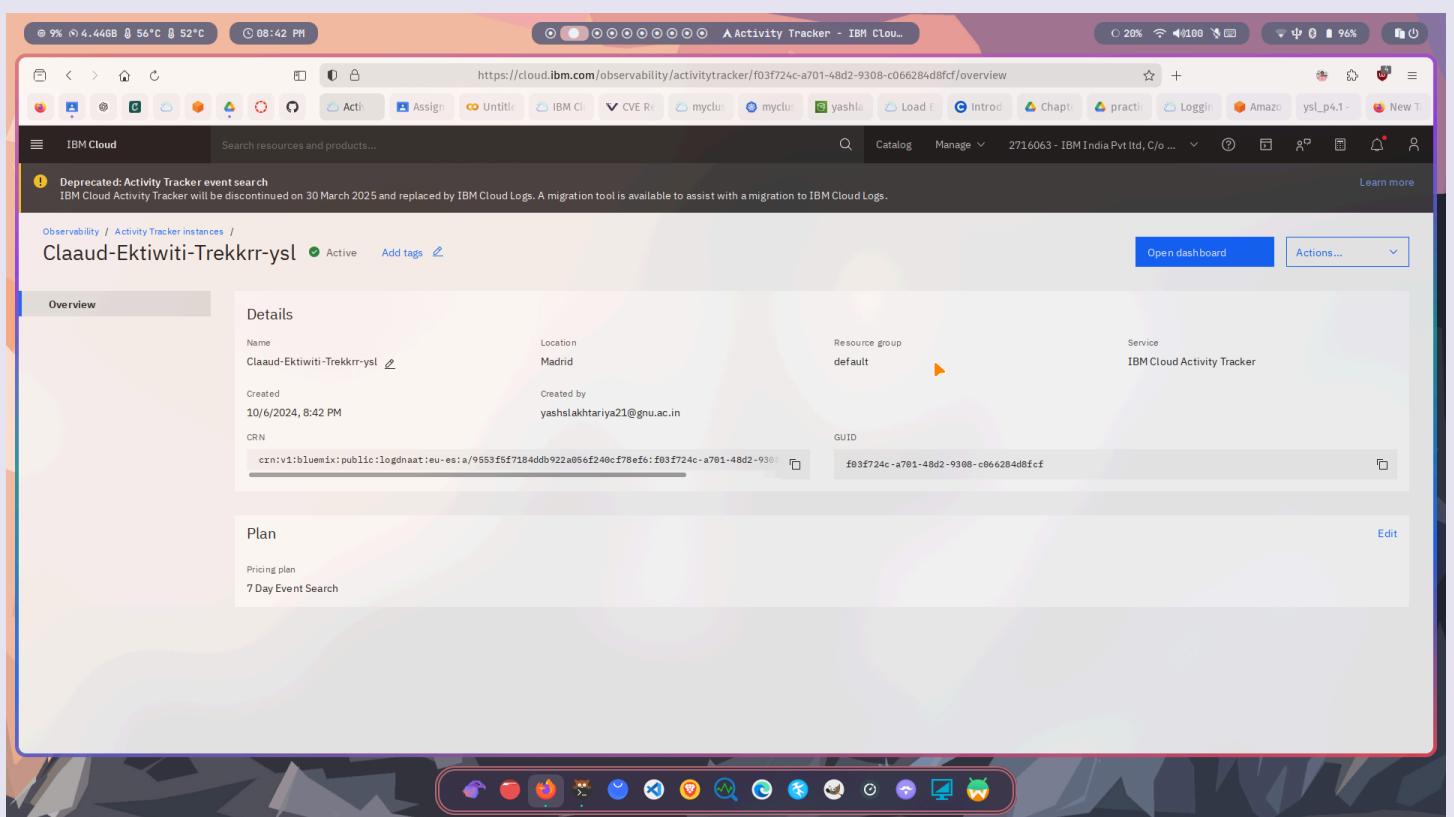
The screenshot shows the IBM Cloud Activity Tracker catalog page. It displays two main service offerings:

- 30 Day Event Search**: Full featured keyword natural language search. Multi-channel Alerting (Pagerduty, Slack, Email, Webhooks etc.), Export API, Archiving, PCI, SOC2, Privacy Shield Compliance, 14 day event search. Priced at ₹269.86381744 INR/Gigabyte-Month.
- HIPAA 30 Day Log Search**: Full featured keyword natural language search. Multi-channel Alerting (Pagerduty, Slack, Email, Webhooks, etc.), Export API, Archiving, HIPAA, PCI, SOC2, Privacy Shield Compliance, 30 day event search. Priced at ₹359.81842325 INR/Gigabyte-Month.

On the right side, there is a **Summary** box containing the following details:

- Cloud Activity Tracker**
- Location:** Madrid
- Plan:** 7 Day Event Search
- Service name:** Claaud-Ektiwiiti-Trekkr-ysl
- Resource group:** default

Below the summary, there are buttons for **Apply promo code**, **Create**, and **Add to estimate**. A checkbox for accepting license agreements is also present.



The screenshot shows the overview page for the IBM Cloud Activity Tracker instance named "Claaud-Ektiwiiti-Trekkr-ysl".

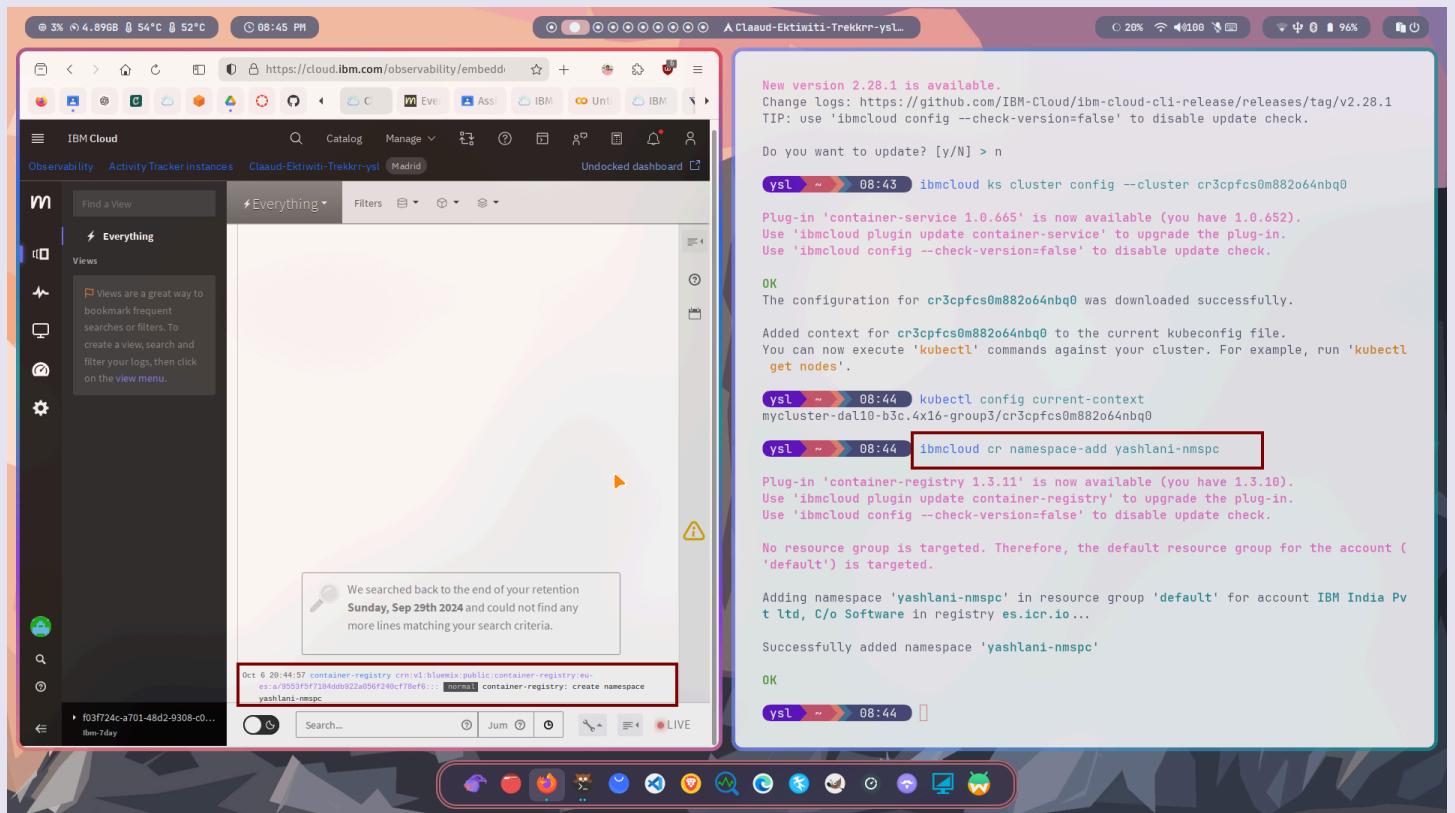
Overview tab is selected. Key details shown include:

- Name:** Claaud-Ektiwiiti-Trekkr-ysl
- Location:** Madrid
- Resource group:** default
- Service:** IBM Cloud Activity Tracker
- Created:** 10/6/2024, 8:42 PM
- Created by:** yash.lakhtariya21@gnu.ac.in
- CRN:** crn:v1:bluemix:public:logDNAat:eu-es:a:9853f5f7184db922a056f240cf78ef6:f03f724c-a701-48d2-9308-c066284d8fcf
- GUID:** f03f724c-a701-48d2-9308-c066284d8fcf

Plan tab is also visible, showing a **Pricing plan** of "7 Day Event Search".

Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 71
CS Assignment 1

2. Now perform operations in container registry to check its logs in that service,
Check and ensure the regions of both services



Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 71
CS Assignment 1

New version 2.28.1 is available.
Change logs: <https://github.com/IBM-Cloud/ibm-cloud-cli-release/releases/tag/v2.28.1>
TIP: use 'ibmcloud config --check-version=false' to disable update check.

Do you want to update? [y/N] > n

```
ysl ~ 08:43 ibmcloud ks cluster config --cluster cr3cpfc0m882o64nbq0
Plugin 'container-service 1.0.665' is now available (you have 1.0.652).
Use 'ibmcloud plugin update container-service' to upgrade the plugin.
Use 'ibmcloud config --check-version=false' to disable update check.
```

OK
The configuration for cr3cpfc0m882o64nbq0 was downloaded successfully.

Added context for cr3cpfc0m882o64nbq0 to the current kubeconfig file.
You can now execute 'kubectl' commands against your cluster. For example, run 'kubectl get nodes'.

```
ysl ~ 08:44 kubectl config current-context
mycluster-dal10-b3c.4x16-group3/cr3cpfc0m882o64nbq0
ysl ~ 08:44 ibmcloud cr namespace-add yashlani-nmspc
```

Plugin 'container-registry 1.3.11' is now available (you have 1.3.10).
Use 'ibmcloud plugin update container-registry' to upgrade the plugin.
Use 'ibmcloud config --check-version=false' to disable update check.

No resource group is targeted. Therefore, the default resource group for the account ('default') is targeted.

Adding namespace 'yashlani-nmspc' in resource group 'default' for account IBM India Pvt Ltd, C/o Software in registry es.icr.io...

Successfully added namespace 'yashlani-nmspc'

OK

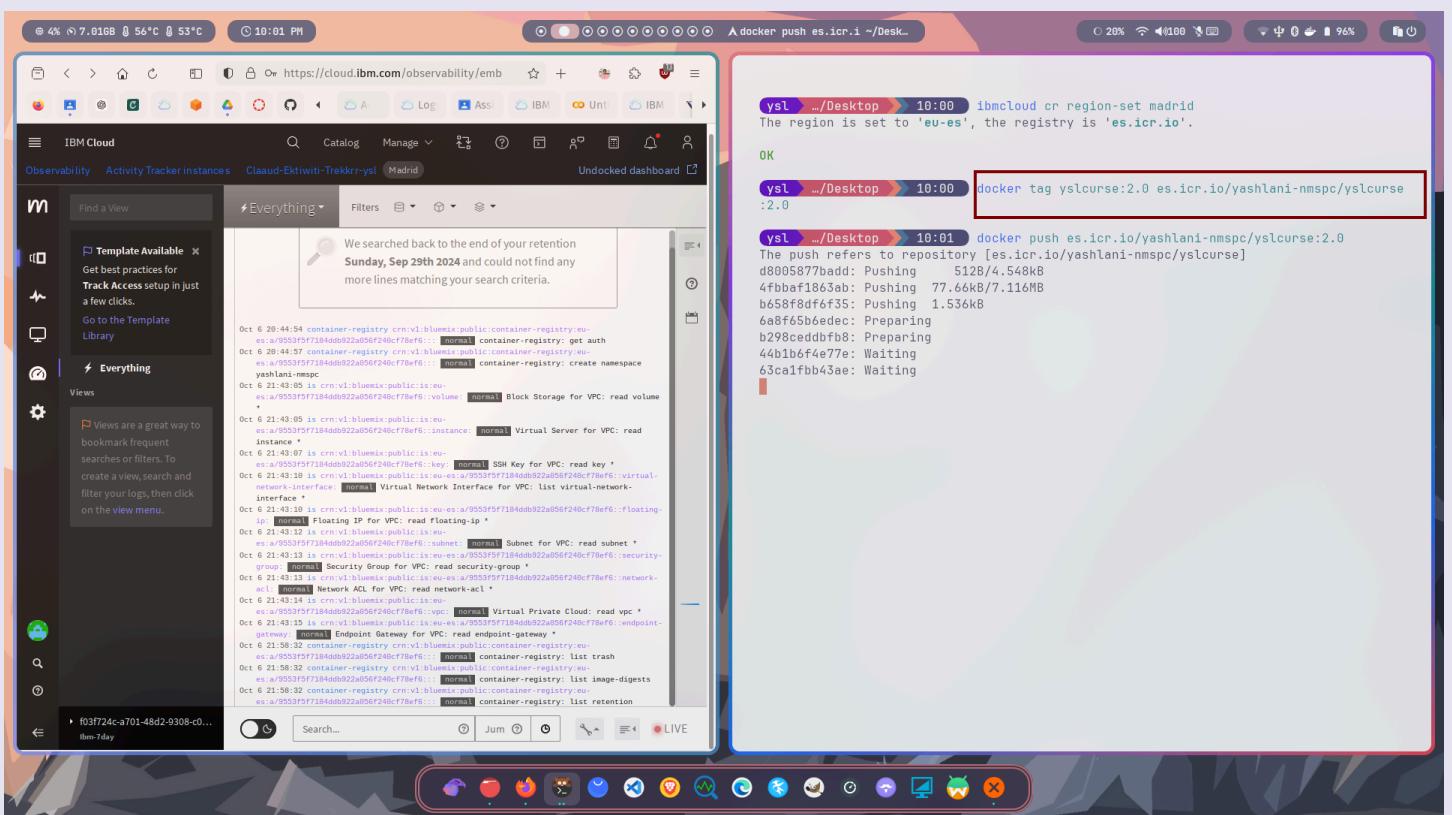
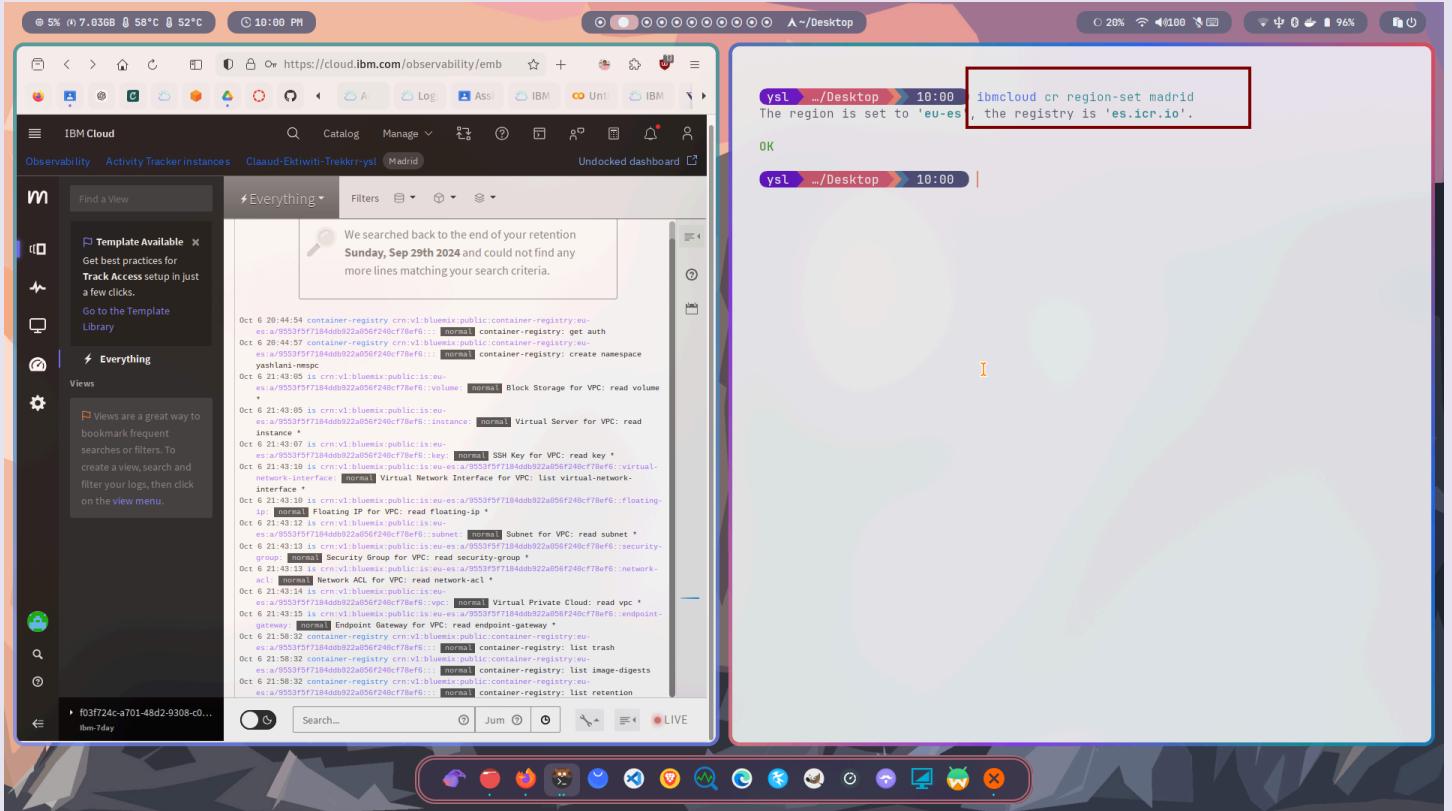
[+] Building 7.5s (4/8)
internal load build definition from Dockerfile
internal load metadata for docker.io/library/node:alpine
internal load .dockerignore
transferring context: 2B
[1/4] FROM docker.io/library/node:alpine@sha256:c9bb43423a6229aeaddf3d16ae6a
internal resolve docker.io/library/node:alpine@sha256:c9bb43423a6229aeaddf3d16ae6a
internal sha256:d17475b51f38657035478cb9896cd7c22918758fa22261da 1.39MB / 1.39MB
internal sha256:f7c3a8abc1f98a73ab9d7f52c3f48cb578481267508fba07fffe5 447B / 447B
internal sha256:c9bb43423a6229aeaddf3d16ae6aaa0ff71a0b2951ce18ec8f 6.41kB / 6.41kB
internal sha256:bec02741e59b7f74ddfb1b7bf2013c178bebdb3b5cf841c2 1.72kB / 1.72kB
internal sha256:49643eaafffd3f2efebel6c22ebe662b5df4ad55a5cf35ea 6.38kB / 6.38kB
internal load build context
internal load build context

File Edit Selection View Go Projects LSP Client Sessions Tools Settings Help

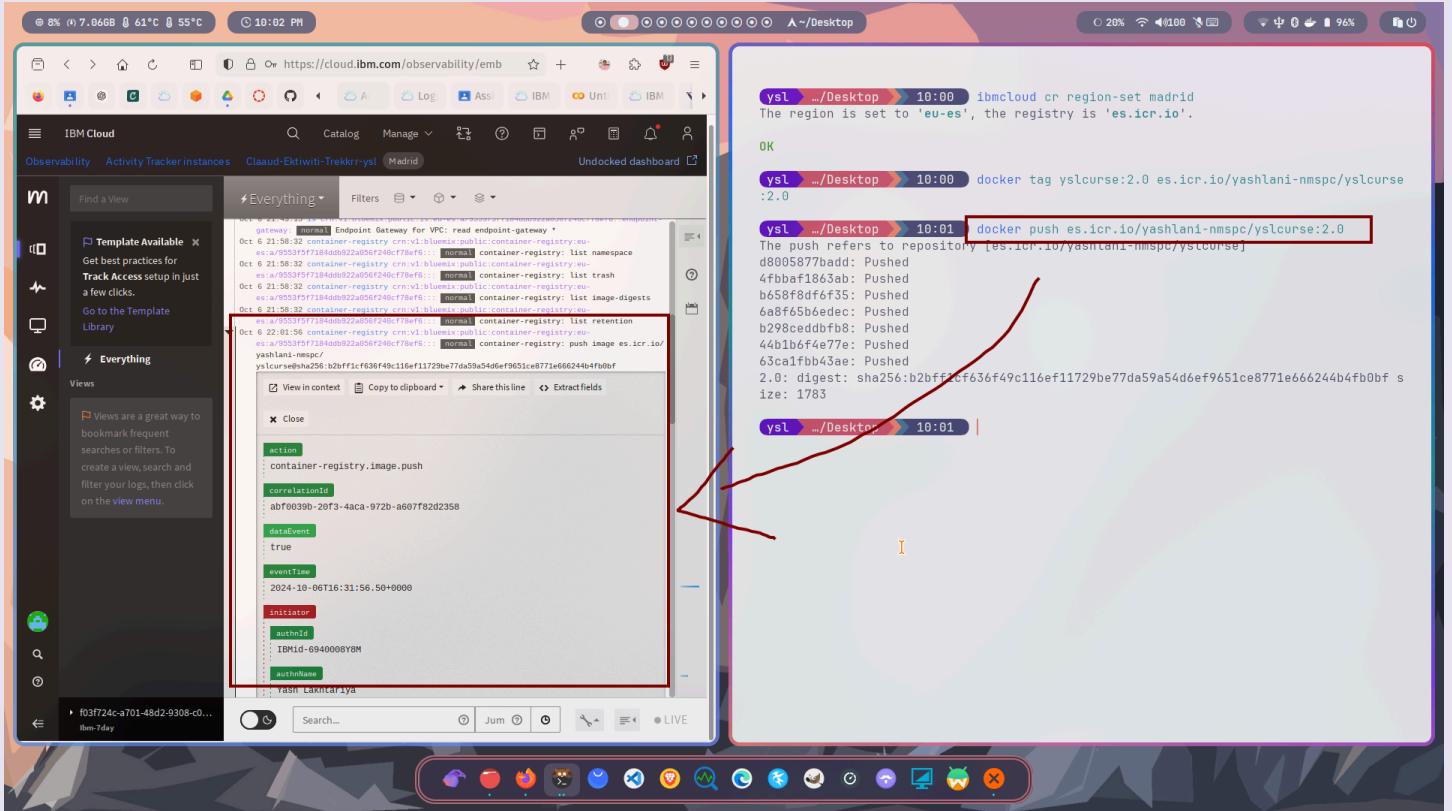
Dockerfile

```
home -> ysl -> Desktop -> Dockerfile
1  FROM node:alpine
2  WORKDIR /app
3  RUN npm install express
4  COPY curse.html /app/curse.html
5  EXPOSE 3000
6  CMD ["sh", "-c", "node -e \'\\
7    const express = require(\"express\")\\';
8    const path = require(\"path\")\\';
9    const app = express();\\';
10   app.use(express.static(path.join(__dirname)));\\';
11   app.get(\"/\", (req, res) => res.sendFile(path.join(__dirname, \"curse.html\")));\\';
12   app.listen(3000, () => console.log(\"Server running on port 3000\"));\\';
13   \'"]
14
```

Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 71
CS Assignment 1



Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 71
CS Assignment 1



Terminal window:

```
ysl ~/Desktop > 10:00 ibmcloud cr region-set madrid
The region is set to 'eu-es', the registry is 'es.icr.io'.

OK

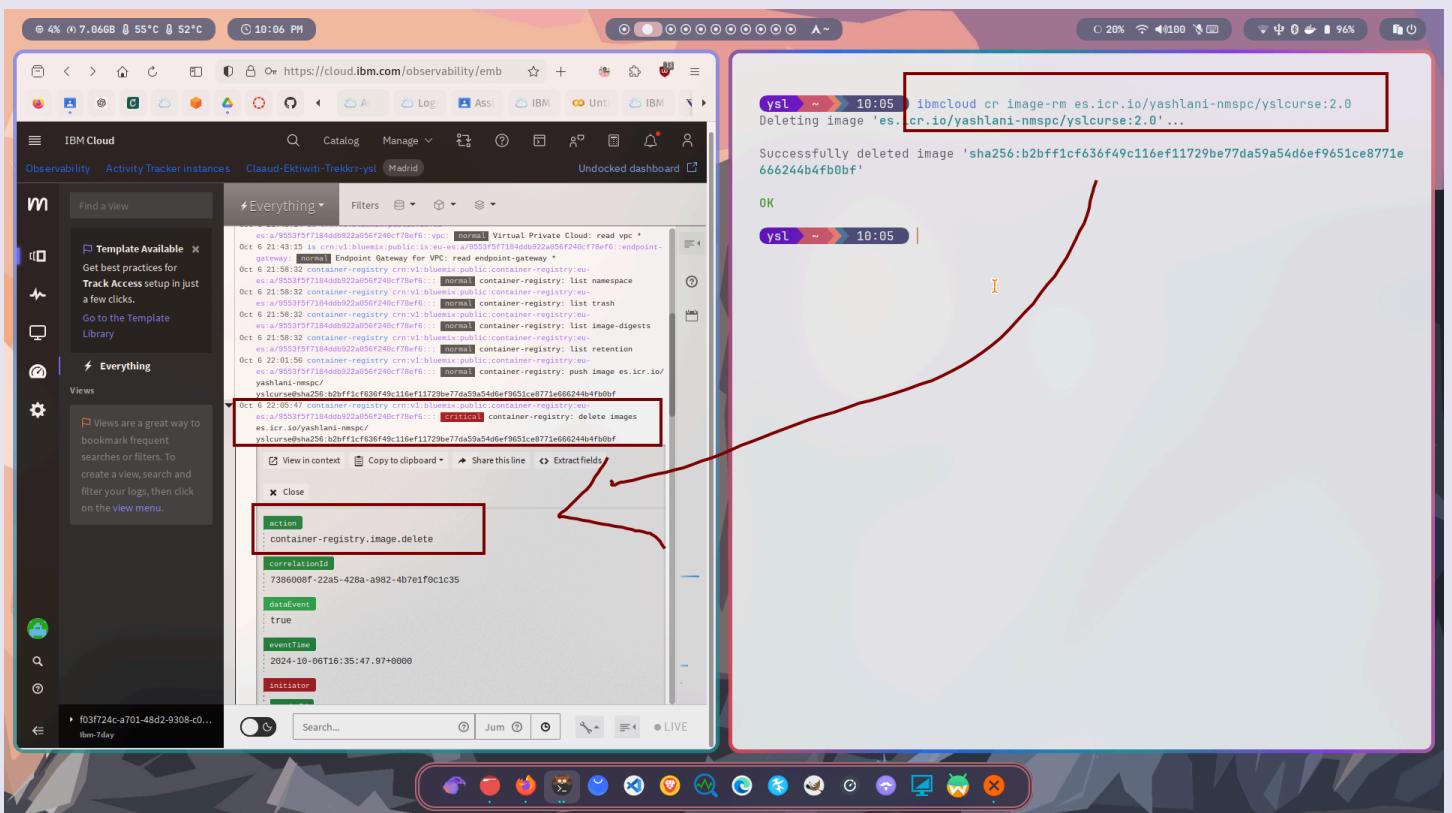
ysl ~/Desktop > 10:01 docker tag yslcourse:2.0 es.icr.io/yashlani-nmspc/yslcourse:2.0
The push refers to repository [es.icr.io/yashlani-nmspc/yslcourse]
d8005877badd: Pushed
4fbba1b63ab: Pushed
b658f8df6f35: Pushed
6abf65b6edec: Pushed
b298ceddbfb8: Pushed
44b1b6f4e77e: Pushed
63c1fbb43ae: Pushed
2.0: digest: sha256:b2bff1cf636f49c116ef11729be77da59a54d6ef9651ce8771e66244b4fb0bf size: 1783

ysl ~/Desktop > 10:01 |
```

Browser window (IBM Cloud Observability):

Logs for Container Registry action: container-registry.image.push

Field	Value
action	container-registry.image.push
correlationId	abf0039b-20f3-4aca-972a-a60ff02d2358
dataEvent	true
eventTime	2024-10-06T16:31:56.50+0000
initiator	<ul style="list-style-type: none">authId: IBMId-6940008YBMauthName: Yash Lakhtariya



Terminal window:

```
ysl ~ 10:05 ibmcloud cr image-rm es.icr.io/yashlani-nmspc/yslcourse:2.0
Deleting image 'es.icr.io/yashlani-nmspc/yslcourse:2.0'...
```

Success message:

```
Successfully deleted image 'sha256:b2bff1cf636f49c116ef11729be77da59a54d6ef9651ce8771e66244b4fb0bf'
```

OK

Terminal window (continued):

```
ysl ~ 10:05 |
```

Browser window (IBM Cloud Observability):

Logs for Container Registry action: container-registry.image.delete

Field	Value
action	container-registry.image.delete
correlationId	7386008f-22a5-428a-a982-4b7e1f0c1c35
dataEvent	true
eventTime	2024-10-06T16:35:47.97+0000
initiator	

Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 71
CS Assignment 1

The screenshot shows two monitors. The left monitor displays the IBM Cloud Observability Activity Tracker interface. It features a sidebar with 'IBM Cloud' and 'Observability' sections, and a main area titled 'Everything' with a log viewer. A specific log entry is highlighted with a red box:

```
Oct 6 22:01:56 container-registry crn:v1:bluemix:public:container-registry:eu-es.icr.io/yashlani-nmspc:yslcurve:2.0:0: Pulling from yashlani-nmspc/yslcurve
Digest: sha256:d2bfff1cf636f749c1ceef11/29b877da59a54d0ef9651ce877ie666244b4fb0bf
Status: Downloaded newer image for es.icr.io/yashlani-nmspc/yslcurve:2.0
es.icr.io/yashlani-nmspc/yslcurve:2.0
```

The right monitor shows a terminal window with a command and its output:

```
ysl ~ 10:12 docker pull es.icr.io/yashlani-nmspc/yslcurve:2.0
2.0: Pulling from yashlani-nmspc/yslcurve
Digest: sha256:d2bfff1cf636f749c1ceef11/29b877da59a54d0ef9651ce877ie666244b4fb0bf
Status: Downloaded newer image for es.icr.io/yashlani-nmspc/yslcurve:2.0
es.icr.io/yashlani-nmspc/yslcurve:2.0
```

Below the terminal, a message says 'What's next: View a summary of image vulnerabilities and recommendations → docker scout quickview es.icr.io/yashlani-nmspc/yslcurve:2.0'.

This screenshot shows the same dual-monitor setup as the previous one. The left monitor displays the IBM Cloud Observability Activity Tracker interface. A different log entry is highlighted with a red box:

```
Oct 6 22:11:35 container-registry crn:v1:bluemix:public:container-registry:eu-es.icr.io/yashlani-nmspc:yslcurve:2.0:0: Pulling from yashlani-nmspc/yslcurve:2.0
Digest: sha256:b2bfffcf636f49c116ef11729be77da59a54d0ef9651ce877ie666244b4fb0bf
Status: Downloaded newer image for es.icr.io/yashlani-nmspc/yslcurve:2.0
es.icr.io/yashlani-nmspc/yslcurve:2.0
```

The right monitor shows a terminal window with a command and its output:

```
ysl ~ 10:14 ibmcloud cr image-list
Listing images...
Repository Size Security status Tag Digest Namespace Created
es.icr.io/yashlani-nmspc/yslcurve 2.0 b2bfffcf636f yashlani-nmspc 20 minutes ago 56 MB -
OK
```

```
ysl ~ 10:14 ibmcloud cr namespace-list
Listing namespaces for account 'IBM India Pvt Ltd' in registry 'es.icr.io'...
Namespace prarthicsexam prathi yashlani-nmspc
OK
```

```
ysl ~ 10:15
```

Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 71
CS Assignment 1

The screenshot shows a dual-monitor setup. The left monitor displays the IBM Cloud Observability Activity Tracker interface, specifically the 'Activity Tracker instances' section. A red box highlights a log entry from 'es.icr.io/yashlani-nmspc' at 10:14, which lists an image named 'yslcurse'. The right monitor shows a terminal window with the command 'ibmcloud cr image-list' at 10:14, listing the same image. Another terminal window at 10:15 shows the command 'ibmcloud cr namespace-list' for the account 'IBM India Pvt Ltd', listing namespaces like 'prarthicsexam', 'prathi', and 'yashlani-nmspc'.

The screenshot shows a dual-monitor setup. The left monitor displays the IBM Cloud Observability Activity Tracker interface. A red box highlights a log entry from 'es.icr.io/yashlani-nmspc' at 10:16, which shows the deletion of the 'yashlani-nmspc' namespace. The right monitor shows a terminal window with the command 'ibmcloud cr namespace-rm yashlani-nmspc' at 10:16, confirming the deletion of the namespace. Another terminal window at 10:17 shows the command 'ibmcloud cr namespace-list' for the account 'IBM India Pvt Ltd', which no longer lists the 'yashlani-nmspc' namespace.