Date
Page No.

Name: Yash Lakhtariya
En no: 211621010 12
Class: 7A (CBA) Batch - 7I
Sub: Cloud Security Assignment - 1

Q - 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 is 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

Date
Page No.

⇒ Measures to ensure cloud security:

(i) Confidentiality:

→ As multiple users are using cloud services & resources, they must remain isolated with each other by provider

→ Only authorized user should be able to access data, implement using Authentication, Authorization through IAM: Roles, Users and 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 POE

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

(iii) Availability:

→ It can be ensured by protection from DOS (Denial of Service) Attacks which disturbs 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.

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

Date
Page No.

Q-2

⇒ 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 Policies.

→ 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 unused data at different location

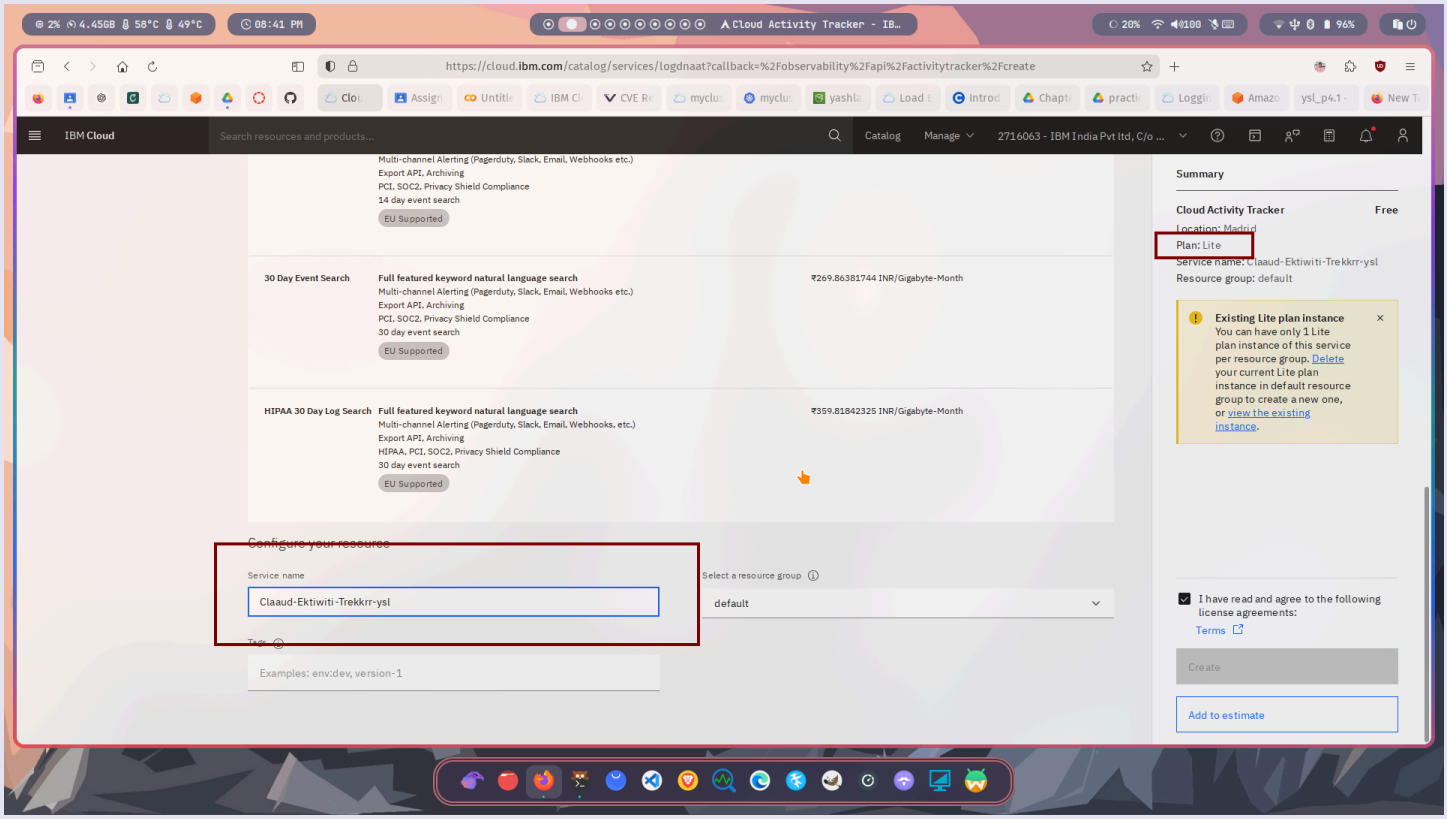
→ For internal-only access, there are different ways:

(i) Used Firewall and company's 'Network & IP only' rules in it.

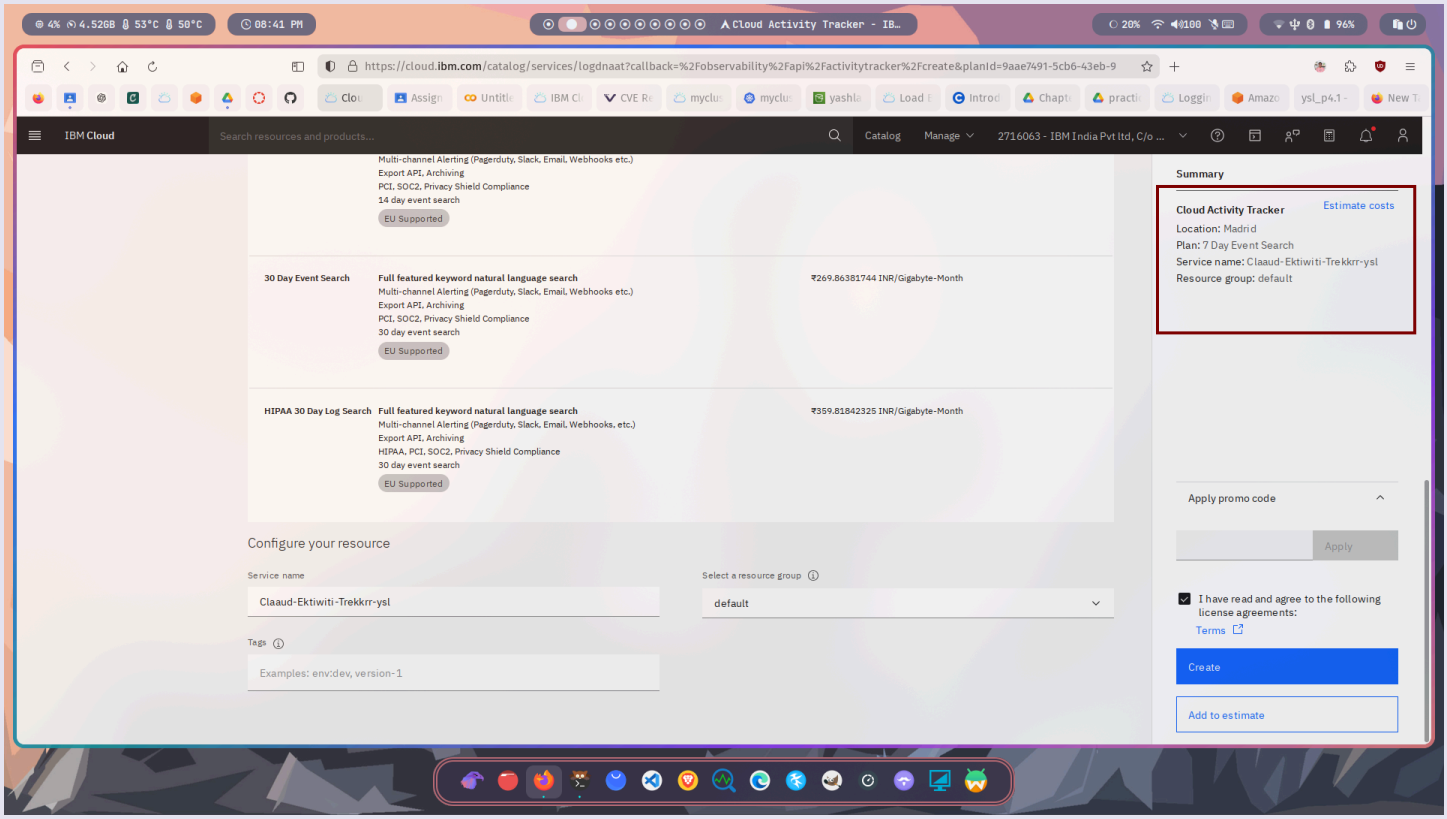
(ii) Create VPC endpoint for bucket and use VPC Gateway Endpoint rules to restrict access.

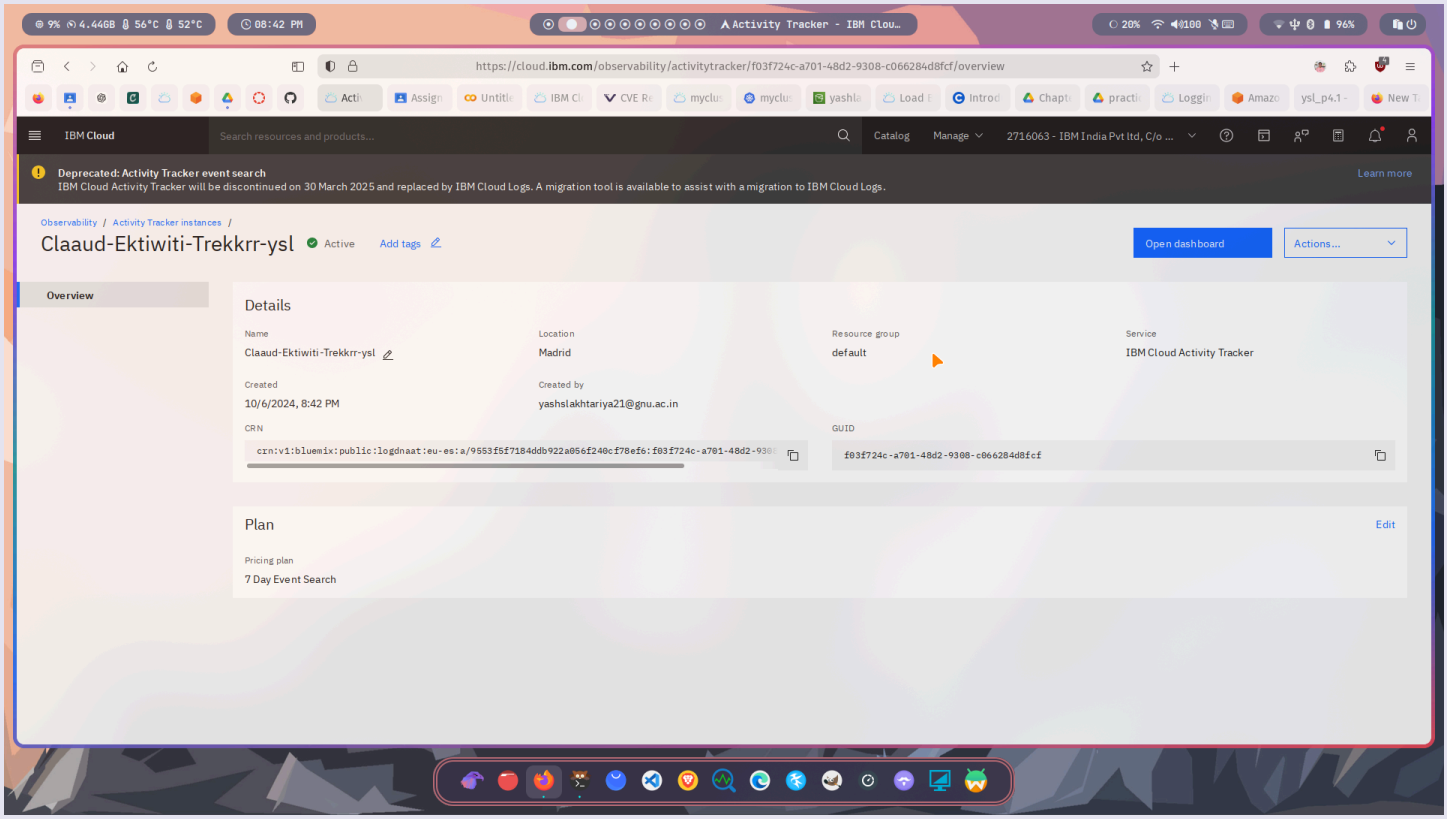
Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 71
CS Assignment 1

1. Create Activity tracker service



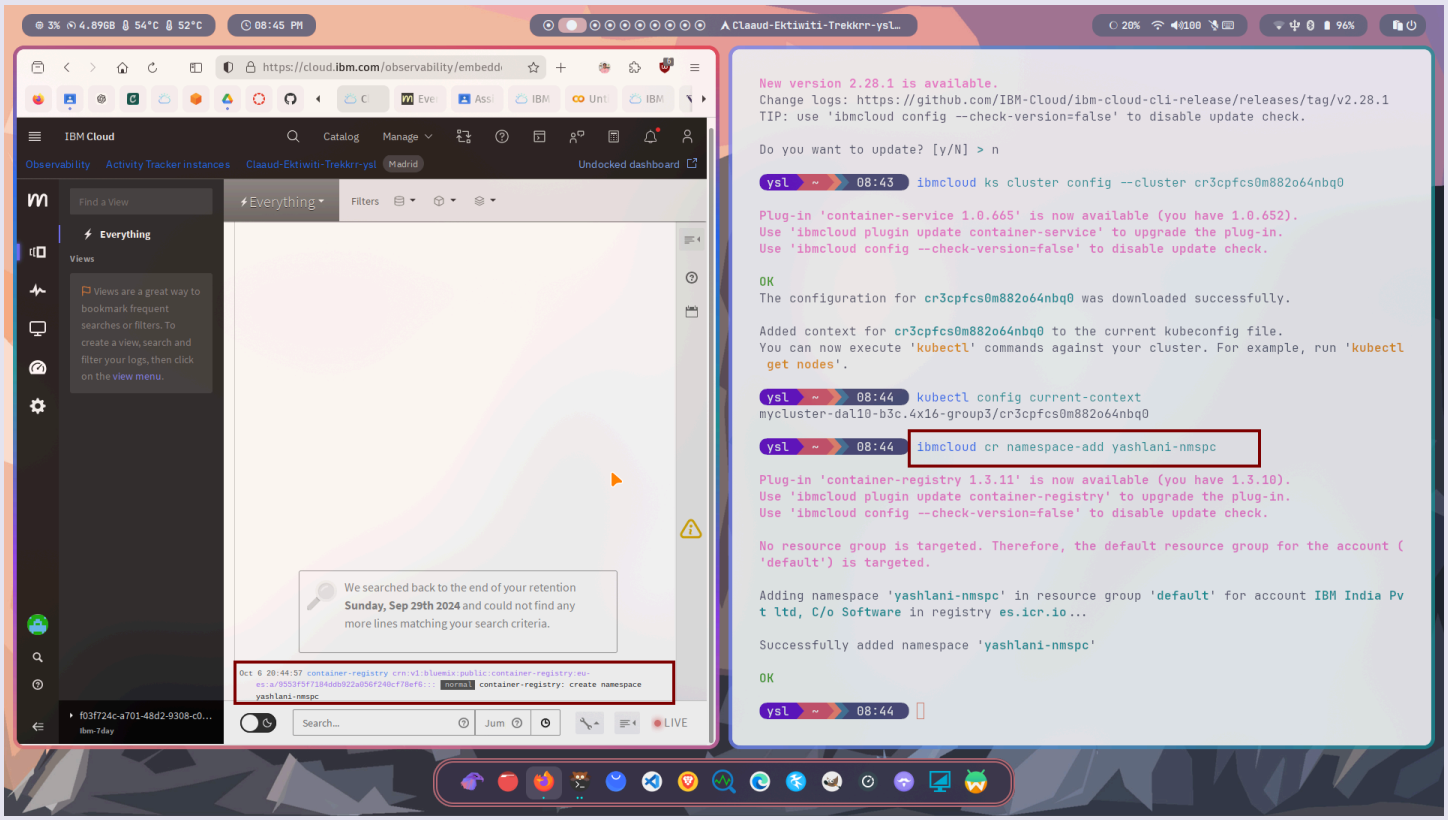
Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 71
CS Assignment 1



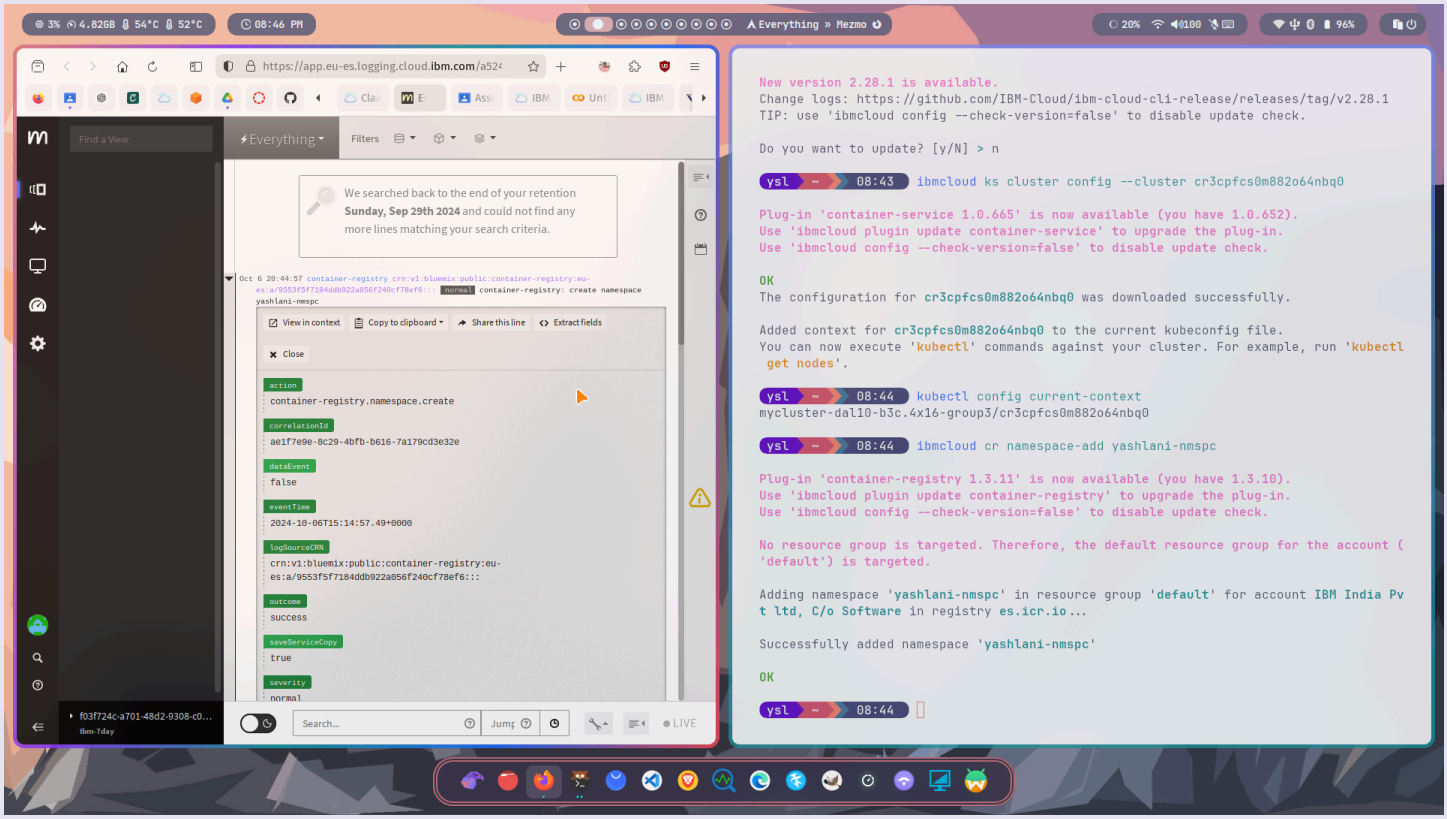


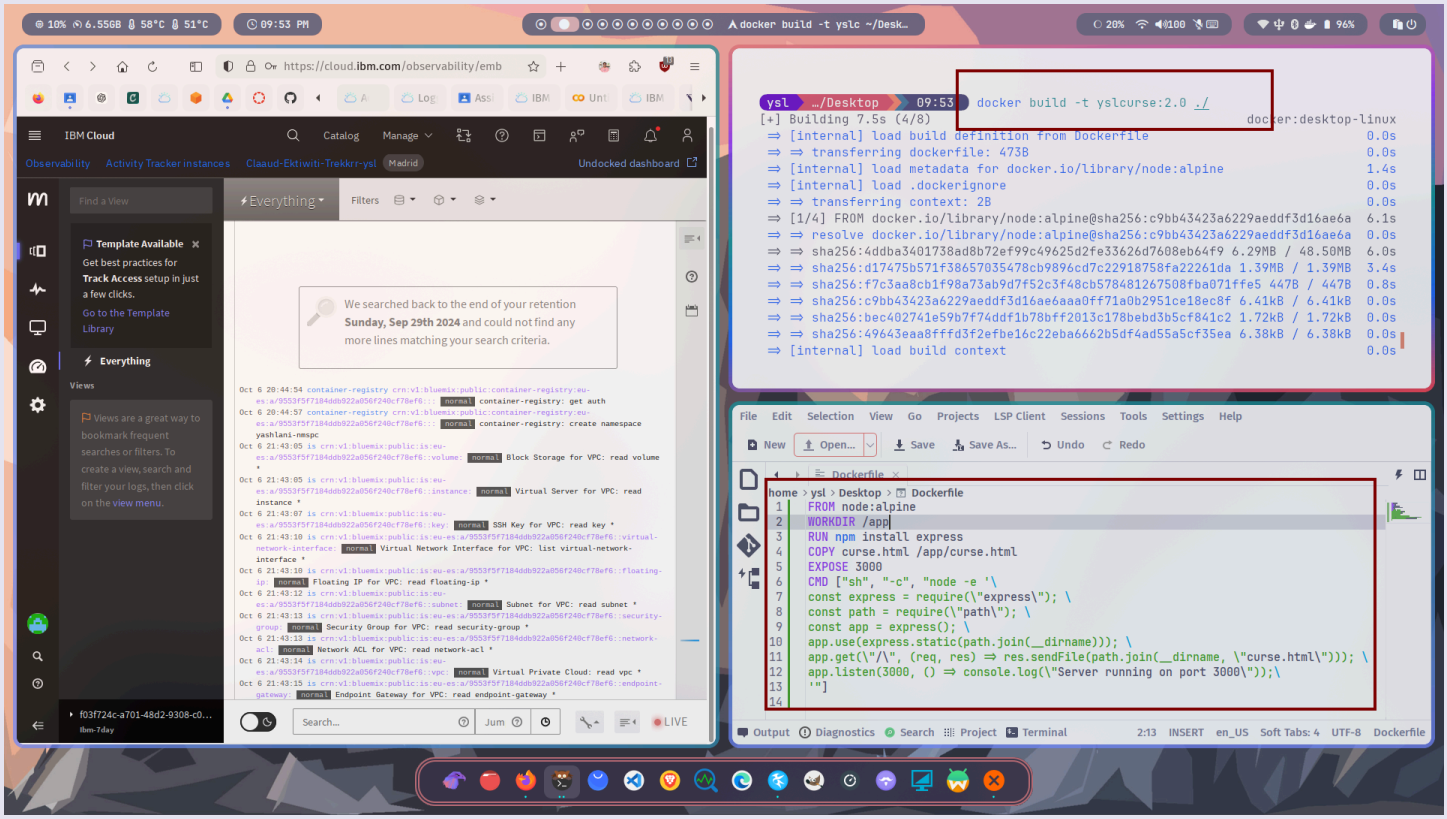
Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 71
CS Assignment 1

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

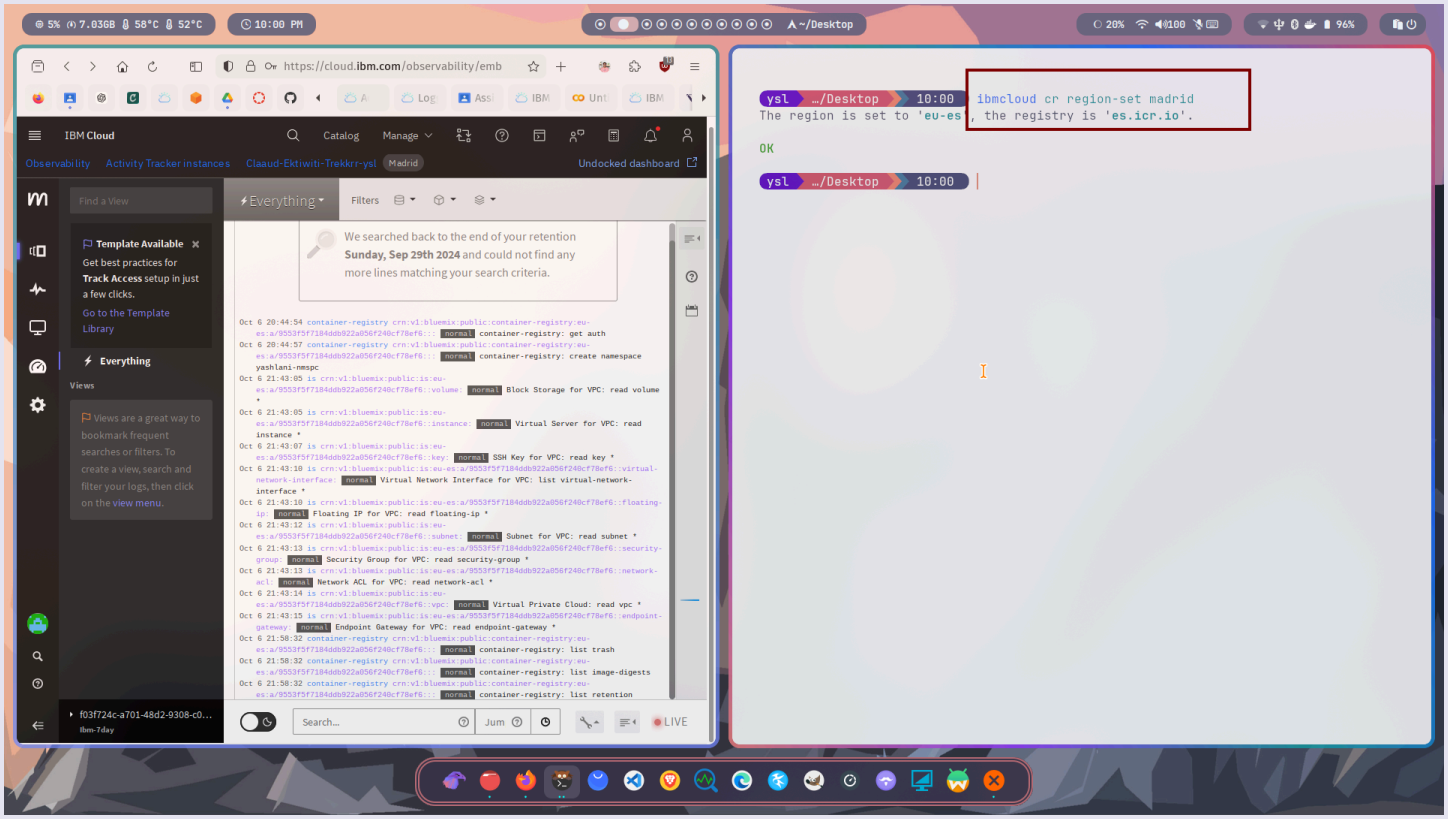


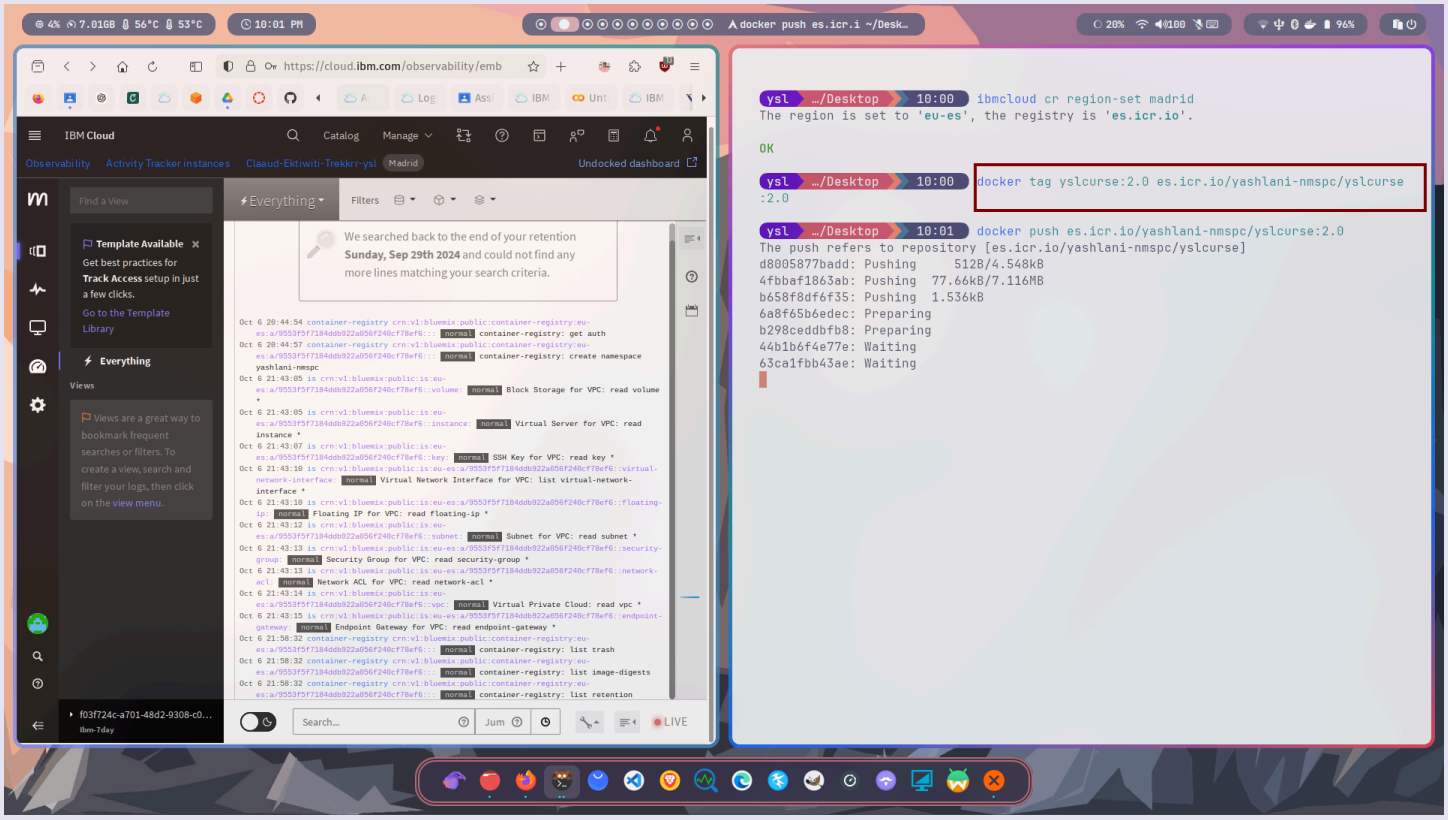
Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 71
CS Assignment 1



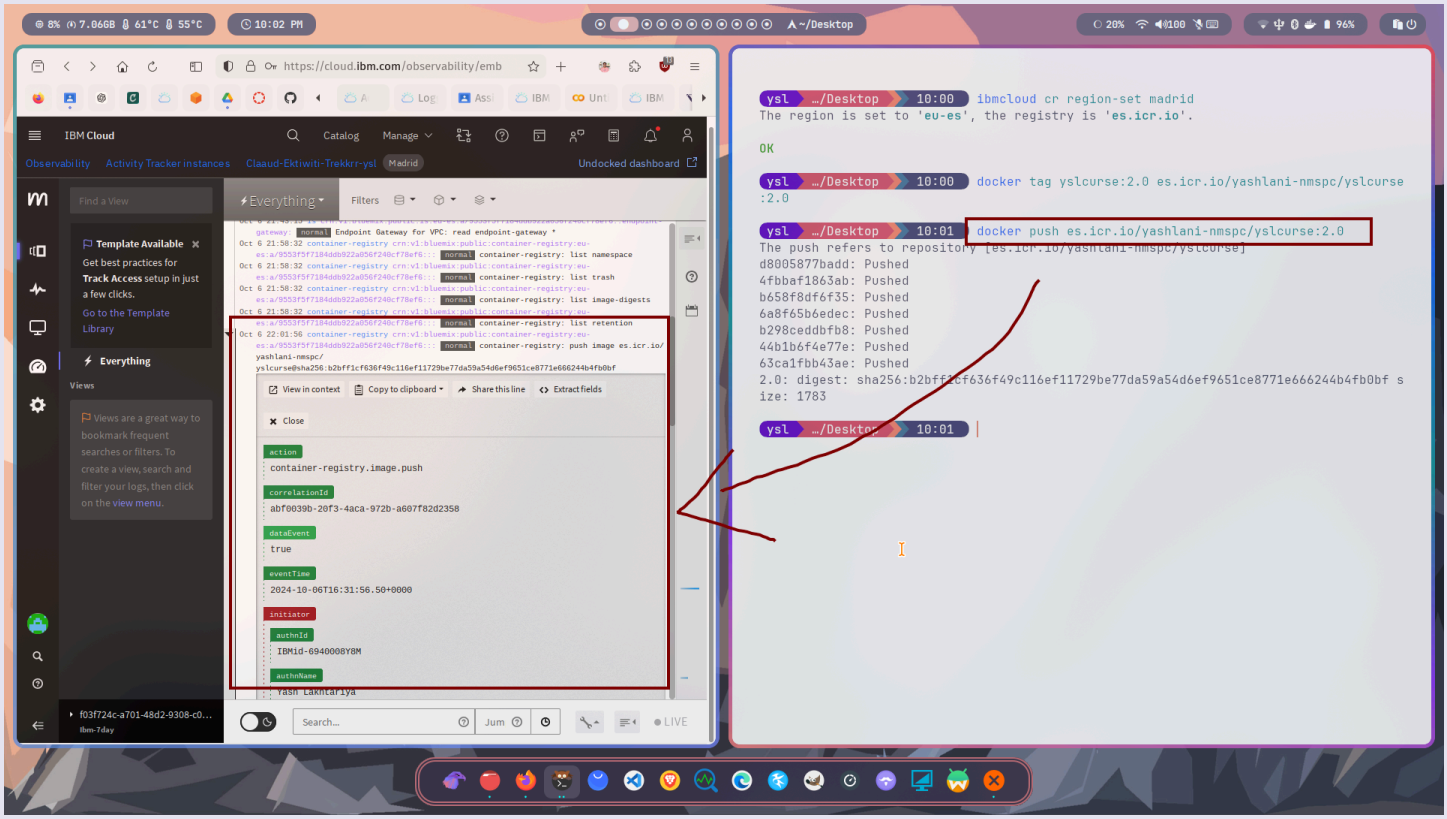


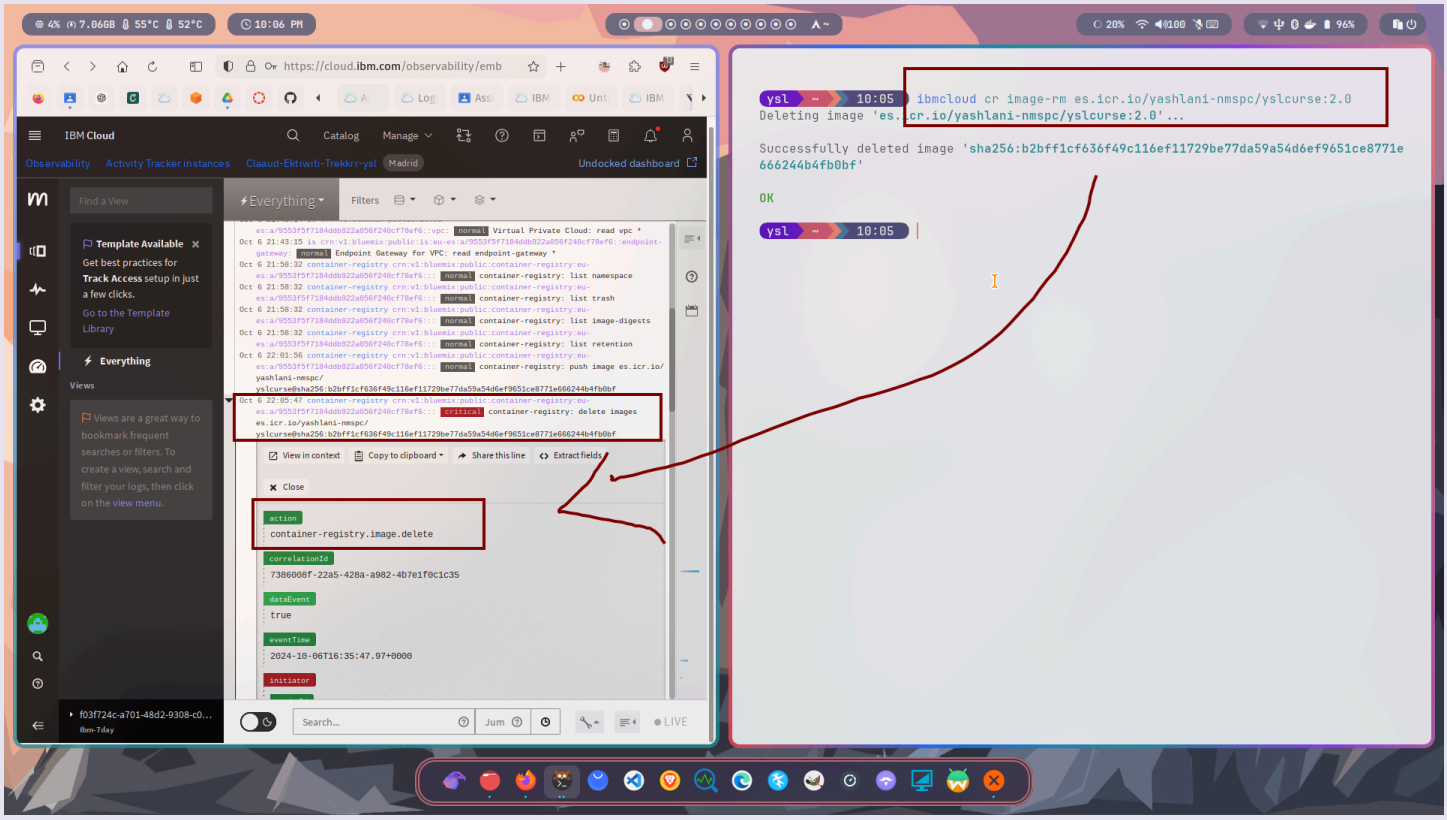
Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 71
CS Assignment 1



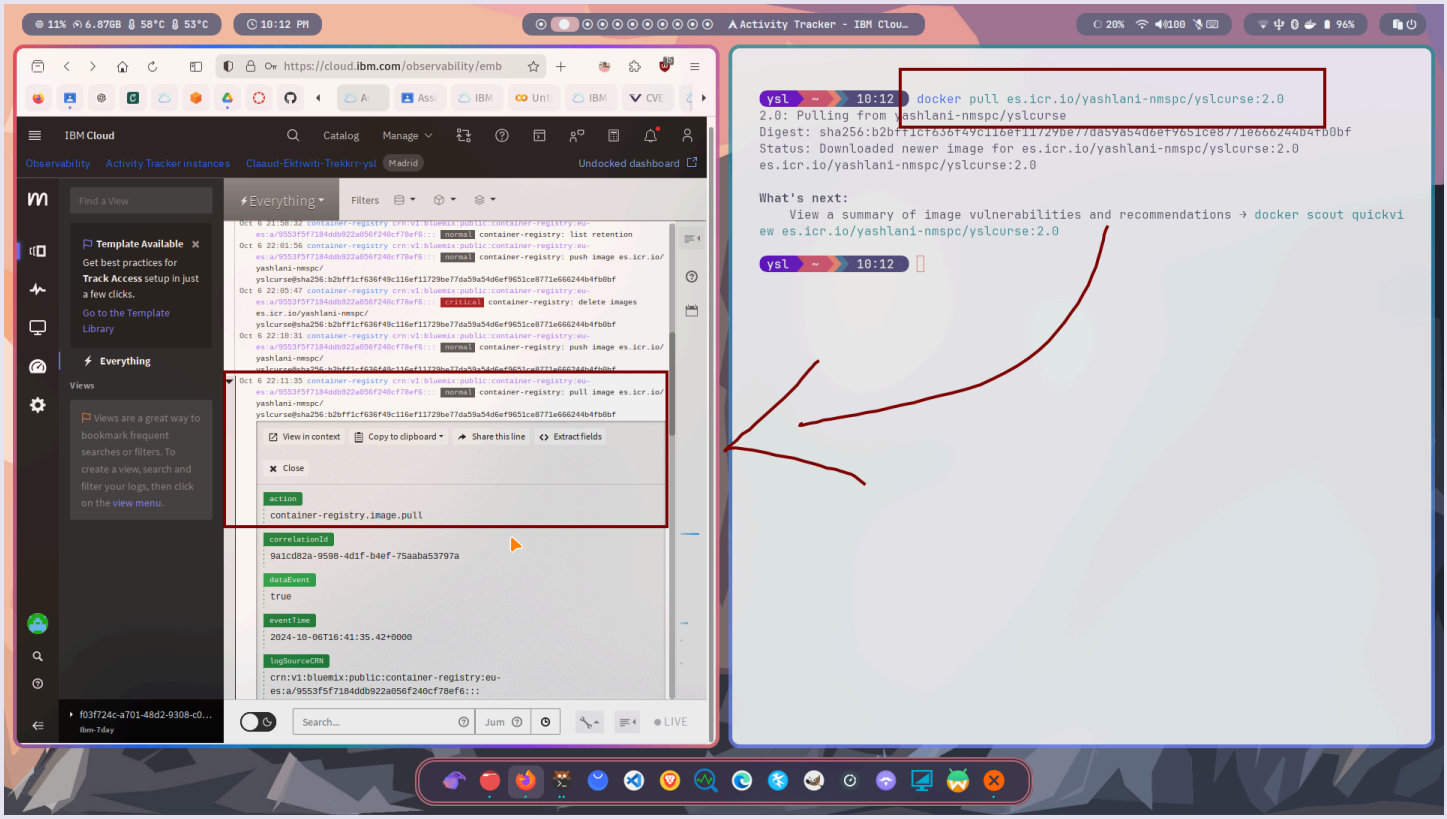


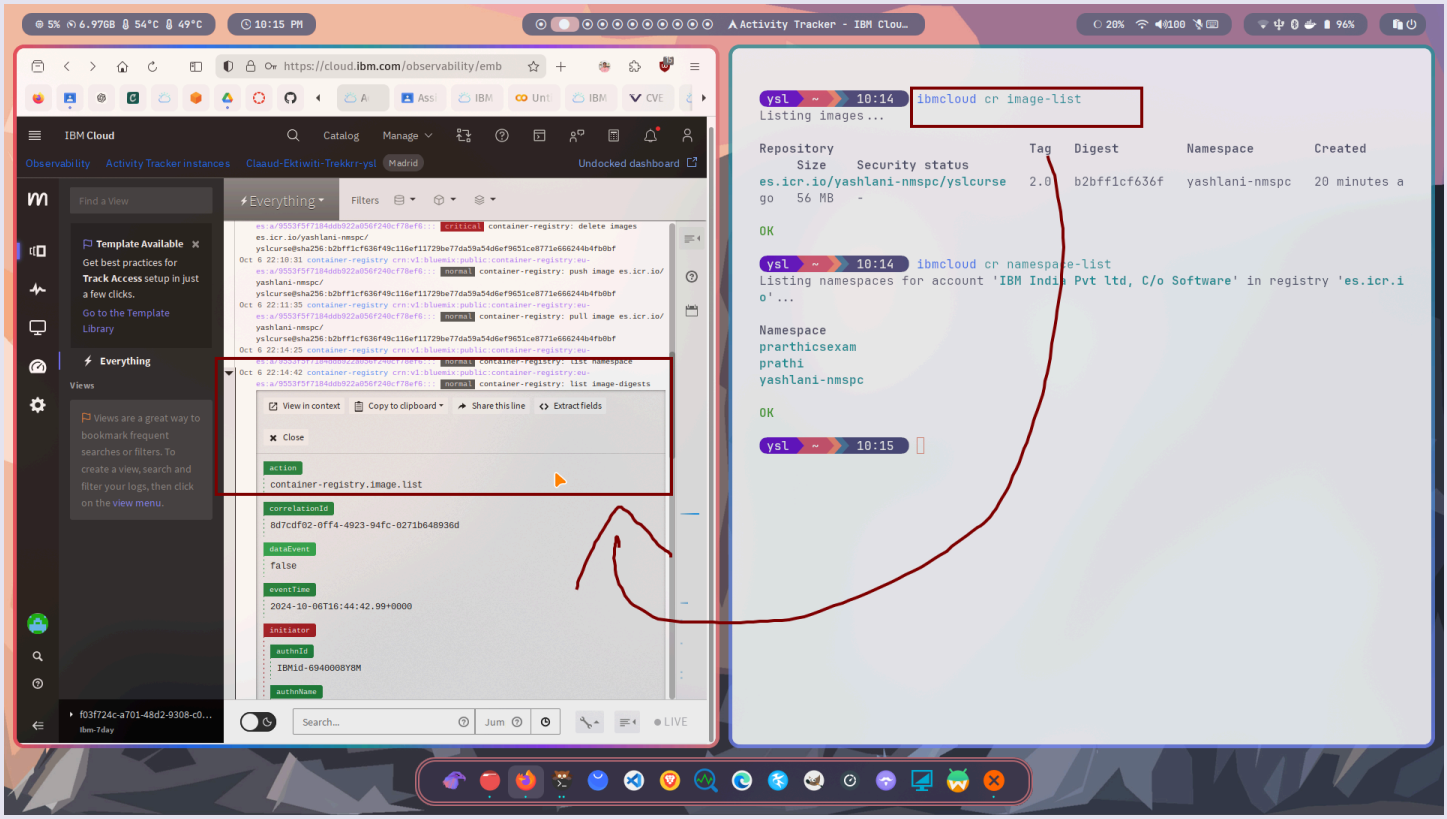
Name - Yash Lakhtariya
Enrollment number - 21162101012
Branch - CBA Batch - 71
CS Assignment 1





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