MIT-WPU

।। विश्वशान्तिर्ध्रुवं ध्रुवा ।।

Dr. Vishwanath Karad
MIT WORLD PEACE UNIVERSITY | PUNE
TECHNOLOGY, RESEARCH, SOCIAL INNOVATION & PARTNERSHIPS

CET4034B: Cloud Infrastructure and Security

SCHOOL OF COMPUTER ENGINEERING AND TECHNOLOGY

T. Y. B. TECH. CSE(CYBERSECURITY AND FORENSICS)

CET4034B: Cloud Infrastructure and Security

Teaching Scheme **Credits: 02 + 01 = 03**
Theory: 2 Hrs. / Week **Practical:** 2 Hrs./Week

Course Objectives

1) Knowledge

i. To study basic cloud computing concepts and its operational environment.

2) Skills

i. To acquire skills of using various Virtualization Techniques and Platforms
ii. To understand challenges in cloud computing

3) Attitude

i. To select and use cloud computing platform

Course Outcomes

After completion of this course students will be able to

i. Setup a cloud environment
ii. Deploy web services efficiently on a cloud platform
iii. Manage cloud services efficiently and effectively
iv. Design, deploy and address the cloud security aspects

Module 4
Security in cloud computing

Disclaimer:

a. Information included in these slides came from multiple sources. We have tried our best to cite the sources. Please refer to the references to learn about the sources, when applicable.

b. The slides should be used only for preparing notes, academic purposes (e.g. in teaching a class), and should not be used for commercial purposes.

Points to be covered

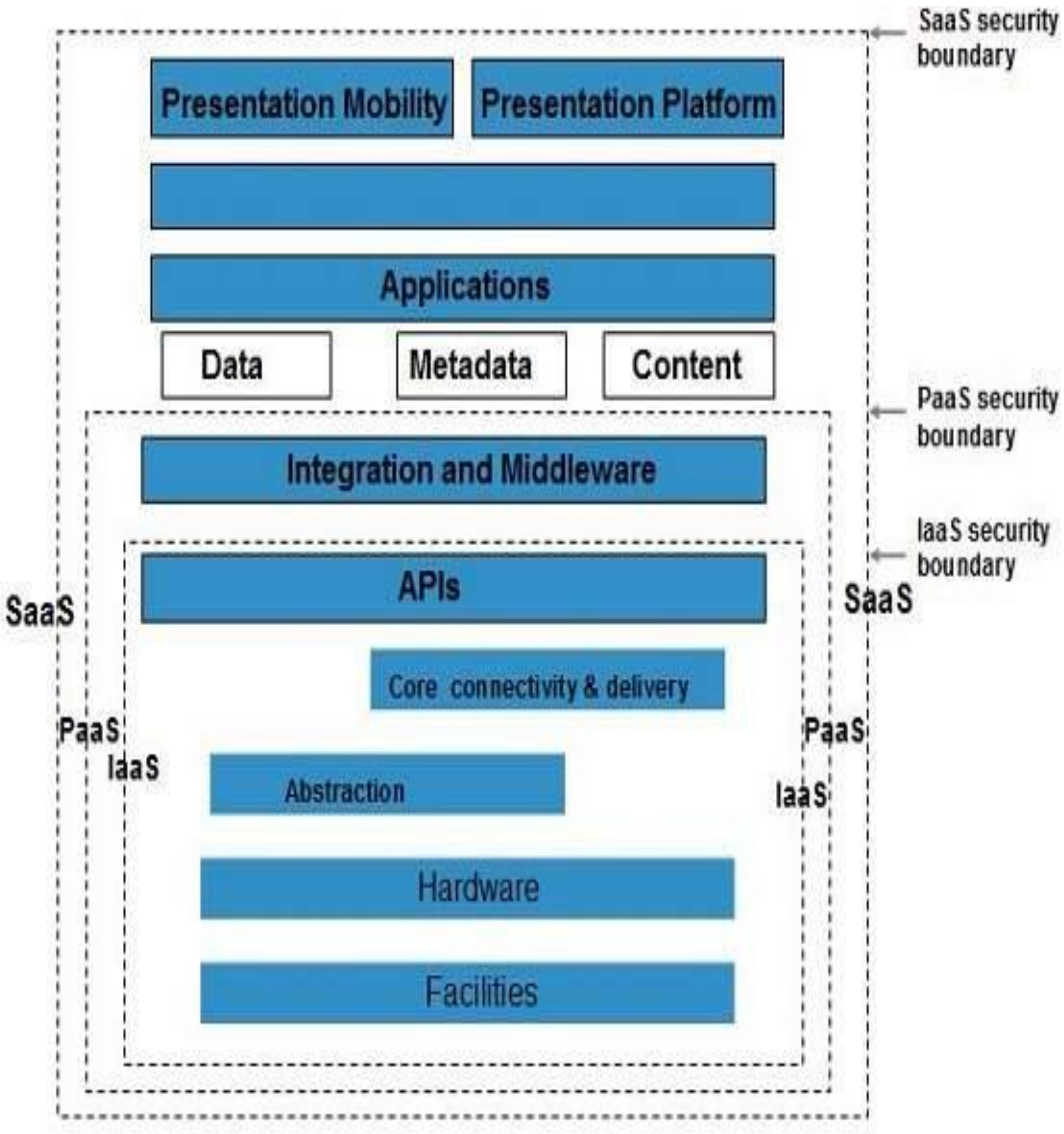
- Introduction to Security in cloud computing
- Global Risk and Compliance aspects in cloud environments
- Key security terminologies
- Digital identity and access management
- Content level security
- Future of Cloud computing:
  - Docker
  - Serverless lambda
  - Micro Services
  - Cloud Forensics

Introduction to Cloud Computing Security

- **Security** in cloud computing is a major concern.
- Data in cloud should be stored in encrypted form.
- To restrict client from accessing the shared data directly, proxy and brokerage services should be employed.
- **Security Planning:** Before deploying a particular resource to cloud, one should need to analyze several aspects of the resource such as:
  - Select resource that needs to move to the cloud and analyze its sensitivity to risk.
  - Consider cloud service models such as **IaaS, PaaS,** and **SaaS.** These models require customer to be responsible for security at different levels of service.
  - Consider the cloud type to be used such as **public, private, community** or **hybrid.**
  - Understand the cloud service provider's system about data storage and its transfer into and out of the cloud.
- The risk in cloud deployment mainly depends upon the service models and cloud types.

Security Boundaries

- A particular service model defines the boundary between the responsibilities of service provider and customer.
- **Cloud Security Alliance (CSA)** stack model defines the boundaries between each service model and shows how different functional units relate to each other.
- The diagram shows the **CSA stack model:**



Key Points to CSA Model

- IaaS is the most basic level of service with PaaS and SaaS next two above levels of services.
- Moving upwards, each of the service inherits capabilities and security concerns of the model beneath.
- IaaS provides the infrastructure, PaaS provides platform development environment, and SaaS provides operating environment.
- IaaS has the least level of integrated functionalities and integrated security while SaaS has the most.
- This model describes the security boundaries at which cloud service provider's responsibilities end and the customer's responsibilities begin.
- Any security mechanism below the security boundary must be built into the system and should be maintained by the customer.
- Although each service model has security mechanism, the security needs also depend upon where these services are located, in private, public, hybrid or community cloud.

Understanding Data Security

- Since all the data is transferred using Internet, data security is of major concern in the cloud.
- Here are key mechanisms for protecting data.
  - Access Control
  - Auditing
  - Authentication
  - Authorization

  - All of the service models should incorporate security mechanism operating in mentioned areas.

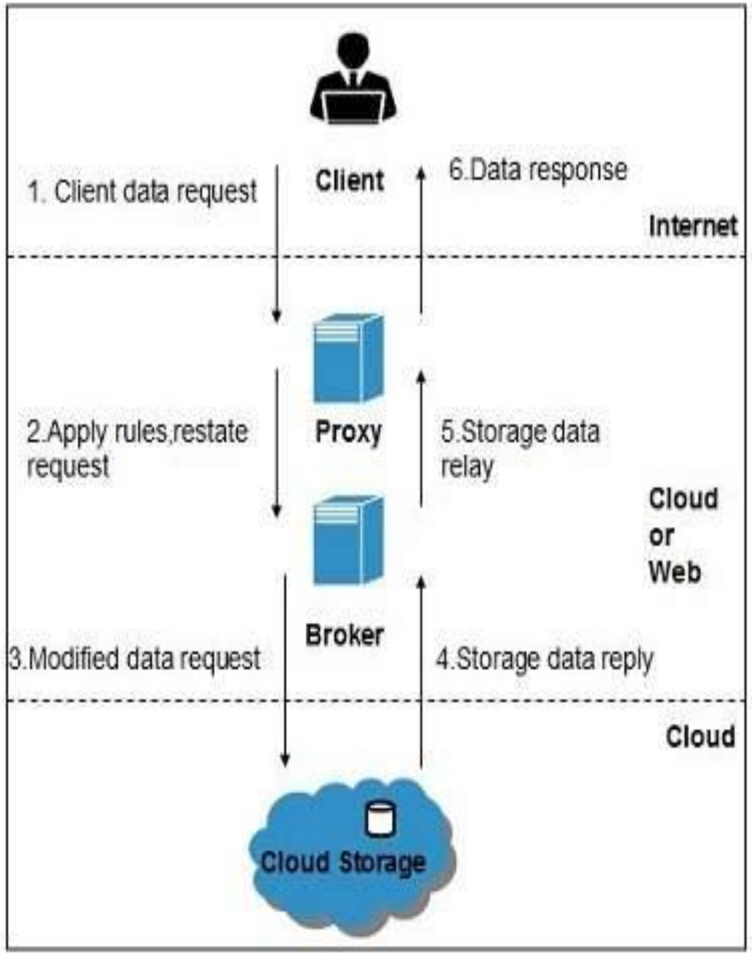
Isolated Access to Data

- Since data stored in cloud can be accessed from anywhere, we must have a mechanism to isolate data and protect it from client’s direct access.
- **Brokered Cloud Storage Access** is an approach for isolating storage in the cloud. In this approach, two services are created:
    - A broker with full access to storage but no access to client.
    - A proxy with no access to storage but access to both client and broker.

Working Of Brokered Cloud Storage Access System

When the client issues request to access data:

- The client data request goes to the external service interface of proxy.
- The proxy forwards the request to the broker.
- The broker requests the data from cloud storage system.
- The cloud storage system returns the data to the broker.
- The broker returns the data to proxy.
- Finally the proxy sends the data to the client.
- All of the above steps are shown in the diagram.



Encryption

- Encryption helps to protect data from being compromised.
- It protects data that is being transferred as well as data stored in the cloud.
- Although encryption helps to protect data from any unauthorized access, it does not prevent data loss.

CLOUD SECURITY – LEGAL,RISK AND COMPLIANCE

- In today's digital era, cloud computing has become a crucial part of business, providing ease, scalability, and cost-effectiveness.
- However, given the increasing dependence on cloud services, it's critical to address the legal risks and compliance issues related with cloud security.
- Here, we investigate the various legal issues that organisations employing cloud technology may encounter and emphasise the need for maintaining compliance in order to secure sensitive data.
- Cloud computing has various advantages, including flexibility, scalability, and lower infrastructure expenses. However, it also introduces unique legal challenges and potential risks that organisations must navigate.
- Cloud security encompasses the strategies, technologies, and practices employed to protect data stored in cloud environments. It involves safeguarding data from unauthorized access, data breaches, data loss, and other security threats. Cloud service providers (CSPs) are in charge of putting security measures in place at the infrastructure, platform, and application levels.

Legal Risks in Cloud Computing

Data Breaches and Privacy Concerns

The risk of data breaches and privacy violations is one of the primary legal threats associated with cloud computing. When organizations store data in the cloud, they entrust the protection of that data to the CSP. A data breach might result in consequences that are legal such as financial loss, reputational harm, and legal responsibility. Furthermore, when personal information is kept or processed in the cloud, it may violate privacy regulations.

Jurisdictional Issues

Cloud computing operates on a global scale, raising jurisdictional challenges. Data stored in the cloud might be subject to the laws and regulations of multiple jurisdictions. Conflicting legal requirements can create complexities in data access, retention, and disclosure. Organizations must carefully apply jurisdictional consideration when selecting a cloud service provider and ensure compliance with applicable laws.

Contractual Obligations

When businesses collaborate with contracts for cloud suppliers of services, those organisations establish contractual relationships which define each party’s rights, responsibilities, and liabilities. Failure to understand the contract’s terms and the legal ramifications might result in disputes, service interruptions, and financial loss. It is essential for organizations to review contracts carefully, negotiate appropriate terms, and ensure compliance with contractual obligations

Compliance Considerations

Regulatory Frameworks

Various regulatory frameworks govern data protection and privacy. Examples include the General Data Protection Regulation
The General Data Protection Regulation (GDPR) in the European Union, the California Consumer Privacy Act (CCPA) in the United States, and the Personal Data Protection Act (PDPA) in Singapore. Understanding and adhering to these regulations is crucial for organizations using cloud services to ensure the lawful processing and protection of personal data.

Data Protection Laws

Data protection laws require organizations to implement appropriate security measures to safeguard personal data. This includes encryption, access controls, regular backups, and secure data transfer protocols. Individuals must also be informed about how their personal information is collected, used, and disclosed by organisations.

Industry-Specific Standards

Certain industries have specific compliance requirements due to the nature of the data they handle. In the United States, for example, healthcare organisations must follow the Health Insurance Portability and Accountability Act (HIPAA), which establishes rules for the protection of patient health information. To protect the security of financial data, financial organisations must follow laws such as the Payment Card Industry Data Security Standard (PCI DSS).

Best Practices for Cloud Security

To mitigate legal risks and enhance cloud security, organizations should adopt the following best practices:

Conducting Due Diligence

Before selecting a cloud service provider, organizations should conduct thorough due diligence. This includes evaluating the provider’s security measures, certifications, and compliance with relevant regulations. It is crucial to assess the provider’s track record, reputation, and data breach incident response capabilities.

Implementing Strong Authentication Measures

Enforcing robust authentication measures, such as multi-factor authentication, helps prevent unauthorized access to cloud resources. Strong passwords, biometric authentication, and access controls based on user roles are effective security measures that organizations should implement.

Regular Monitoring and Auditing

Continuous monitoring and auditing of cloud infrastructure and applications are essential to identify security vulnerabilities, detect potential threats, and ensure compliance. Security logs, intrusion detection systems, and automated security scans can help organizations proactively address security risks.

Cloud computing offers immense benefits, but it also presents legal risks and compliance challenges. Organizations must recognize the importance of addressing these risks by understanding the legal landscape, adhering to relevant regulations, and implementing robust security measures. By taking a proactive approach to cloud security and compliance, businesses can protect their data, maintain customer trust, and mitigate legal liabilities.

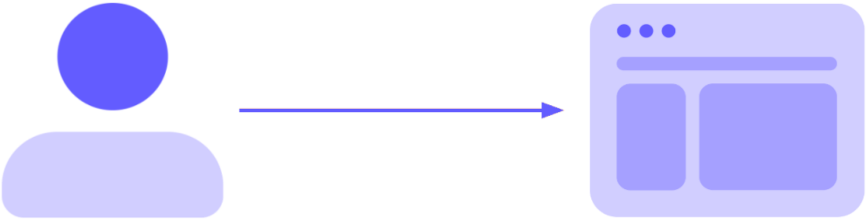
Key strategies for securing your data in the cloud

- **Strengthening IAM Infrastructure:** A well built IAM infrastructure safeguards the cloud data storage and transactions by establishing centralized user management, granular access control and RBAC(Role-based Access Control), Identity Lifecycle Management and strong authentication to cloud services.
- **Advanced Encryption:** Data should be encrypted both in transit and at rest. Implementing advanced encryption mechanisms on the client's side along with the default encryption options provided by the cloud service providers helps protect data even if it is compromised or accessed without authorization. Key management services like AWS Key Management Service (KMS) and Microsoft Azure Key Vault, enables us to create and control the encryption keys used to encrypt your data on the respective platforms..
- **Data Backup and Disaster Recovery:** Ensuring regular data backup and establishing an effective data recovery plan helps in situations where crucial data has been corrupted or lost. Data backup and recovery plan also ensures that there is no interruption in business operations due to data loss. Cloud services like Google Cloud Storage and Microsoft Azure provide backup and recovery services by implementing backups, data compression, geo-redundancy and flexible retention policies.
- **Strong Authentication Layers:** Multi-level authentication to cloud services prevents unauthorized access to some extent even if there is credential leak. For example, MFA(Multi-Factor Authentication) including OTPs, biometric authentication, and hardware authentication, enhance security level for user authentication.
- **Regular Security Audits and Security Assessments:** Identifying vulnerabilities in a cloud infrastructure, applications, and configurations can be done by regular security audits. This can be used in turn to fix the weaknesses that can lead to data breaches in the future. Security Assessments for the CSPs are done to evaluate the security certifications, compliance with standards and incident response capabilities.
- **Implementing DLP Tools:** A Data Loss Prevention (DLP) tool is a security solution designed to prevent the unauthorized disclosure or loss of sensitive data. These tools help identify, classify, monitor, and protect sensitive data, enabling proactive detection and prevention of data breaches, unauthorized access, and data leakage incidents.

4 Pillars of Cloud Security

Cloud security aims to protect more than just the perimeter, bringing security all the way down to the data. Some of the most common measures include:

1. **Identity and access management (IAM)** to help provision access to resources in cloud environments. IAM also helps you prevent unauthorized access to data, apps, and infrastructure shared across clouds.
2. **Data loss prevention (DLP)** to monitor and inspect data to prevent exfiltration. DLP is an essential element of cloud computing security that a traditional security model can't carry out effectively.
3. **Data encryption** to encode data so that attackers can't interpret it without decrypting it. Encryption also helps establish trust and preserve anonymity, and is required by various privacy regulations worldwide.
4. **Security information and event management (SIEM)** to analyze security logs in real time, giving your security team increased visibility over your cloud ecosystem.



A user wants access to a resource.

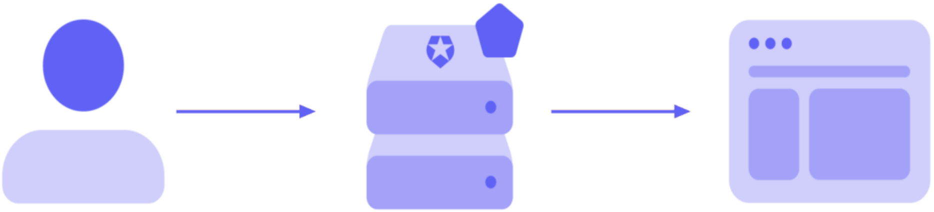
Digital identity and access management

- Identity and access management provides control over user validation and resource access.
- Commonly known as IAM, this technology ensures that the right people access the right digital resources at the right time and for the right reasons.

IAM basic concepts

To understand IAM, you must be familiar with some fundamental concepts:

- A **digital resource** is any combination of applications and data in a computer system. Examples of digital resources include web applications, APIs, platforms, devices, or databases.
- The core of IAM is **identity**. Someone wants access to your resource. It could be a customer, employee, member, participant, and so on. In IAM, a **user** account is a digital identity. User accounts can also represent non-humans, such as software, Internet of Things devices, or robotics.
- **Authentication** is the verification of a digital identity. Someone (or something) authenticates to prove that they're the user they claim to be.
- **Authorization** is the process of determining what resources a user can access.

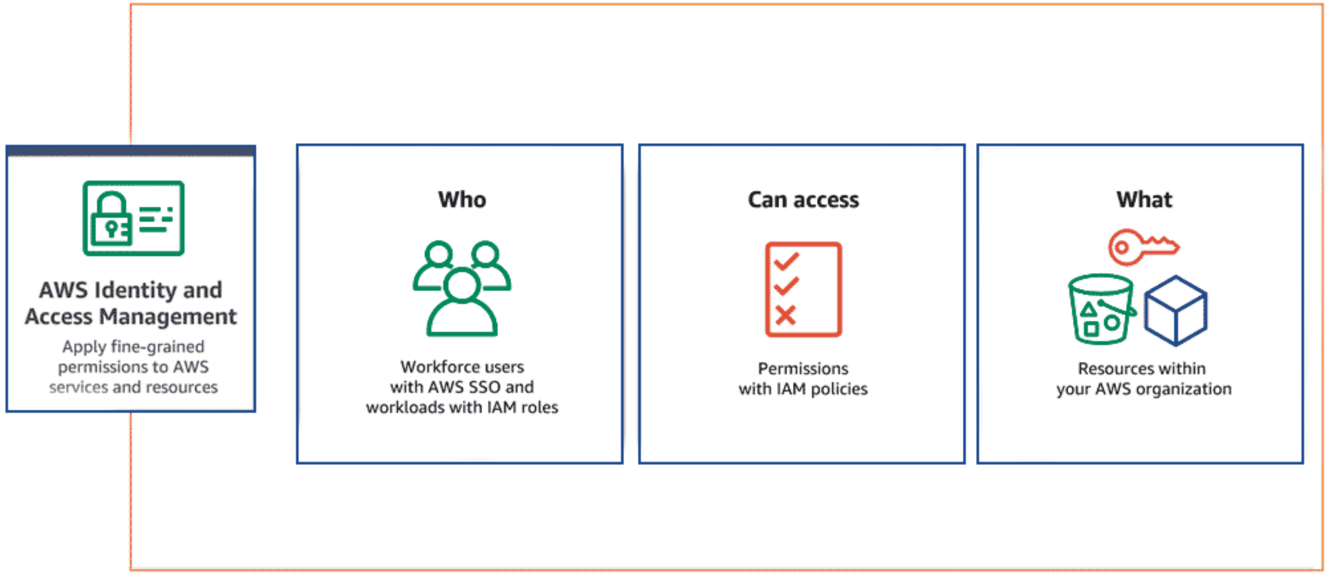


Identity and access management verifies the user and controls their access to the resource.

https://auth0.com/docs/get-started/identity-fundamentals/identity-and-access-management#how-does-iam-work-

How Identity and Access Management Works?

- AWS(Amazon Web Services) will allows you to maintain the fine-grained permissions to the AWS account and the services provided Amazon cloud.
- You can manage the permissions to the individual users or you can manage the permissions to certain users as group and roles will helps you to manage the permissions to the resources.



AWS Identity and Access Management
Apply fine-grained permissions to AWS services and resources

Who
Workforce users with AWS SSO and workloads with IAM roles

Can access
Permissions with IAM policies

What
Resources within your AWS organization

https://www.geeksforgeeks.org/identity-and-access-management/

Content level security

- Content level security is a type of data security that focuses on securing the content of a file or document, rather than just the file itself.

- Content-level security refers to the protection of digital content at a granular level, ensuring that only authorized individuals or systems can access, modify, or distribute specific pieces of content.

- This approach to security focuses on safeguarding the content itself rather than simply securing the infrastructure or network that hosts it.

- Content-level security involves implementing various measures and technologies to enforce access controls, encryption, integrity checks, and other security mechanisms directly on the content.

Key aspects and features of content-level security

1. **Access Controls:** Content-level security implements access policies to regulate who can access specific content and under what conditions.

2. **Encryption:** Utilizes encryption algorithms to encode content, ensuring it remains protected from unauthorized access or interception during transit and while at rest.

3. **Digital Rights Management (DRM):** DRM technologies control the usage and distribution of digital content by enforcing restrictions on copying, sharing, printing, etc., based on predefined rules and policies.

4. **Data Loss Prevention (DLP):** DLP solutions monitor and control the flow of data within an organization's network, preventing unauthorized disclosure or leakage of sensitive information.

5. **Integrity Verification:** Content-level security verifies the integrity of digital content using techniques like checksums, digital signatures, or cryptographic hashes to detect unauthorized modifications or tampering.

6. **Watermarking:** Embeds imperceptible identifiers or marks into digital content to uniquely identify its origin or owner, deterring unauthorized copying or distribution of copyrighted material.

Pros of content-level security

1. **Granular control:** With content level security, it is possible to provide more granular control over who can access specific parts of a document or file,which can be particularly useful in regulated industries or when dealing with sensitive data

2. **Increased security:** By focusing on securing the content of a file or document,content level security can provide a higher level of security than traditionalfile-level security approaches, which only protect the file itself.

3. **Easy to implement:** Many modern content management systems and other enterprise applications include built-in content level security features that are easy to configure and manage.

Cons of content-level security

1. **Performance overhead:** Content level security can add an overhead in terms of performance, particularly when dealing with large files or complex documents. This can impact the speed and responsiveness of applications and systems that need to process these files.

2. **Complexity:** Implementing and managing content level security can be more complex than traditional file-level security approaches. It may require additional expertise, training, and resources.

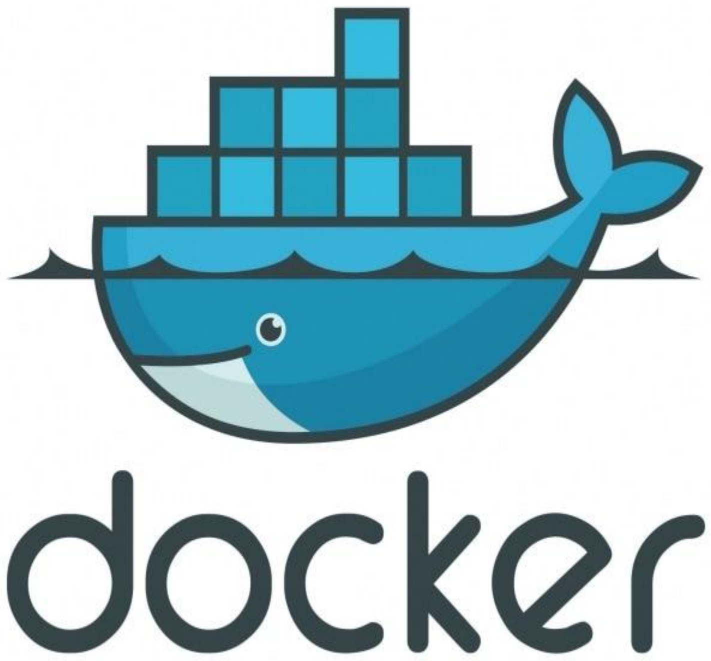
3. **Risk of over complication:** With content level security, it can be easy to overcomplicate the security measures and make it difficult to access, edit, orshare the files or documents, which can hinder productivity

Future of Cloud Computing

Docker,Serverless Lambda,Microservices,Cloud Forensics

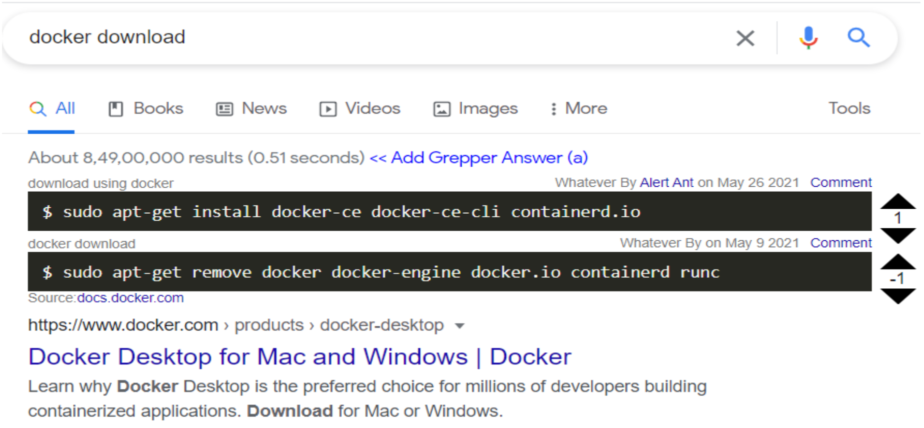
Docker

- Docker is an **open platform for developing, shipping, and running applications in containers,** which are lightweight and portable environments that contain everything needed to run the application, including the code, runtime, libraries, and dependencies.
- Benefits of docker containers include **Consistency, Portability, Efficiency,Scalability and isolation.**
- It is extensively used in **Software development,Big Data and Analytics,IoT and Edge Computing,ML and AI**



Docker installation steps

Step 1: For installation of Docker, go to your favorite browser(chrome will be used here, but it can be done by using any browser). In the search bar, type Docker download. And click on the first link that appears.



About 8,49,00,000 results (0.51 seconds) << Add Grepper Answer (a)

download using docker — Whatever By Alert Ant on May 26 2021 Comment

```
$ sudo apt-get install docker-ce docker-ce-cli containerd.io
```

docker download — Whatever By on May 9 2021 Comment

```
$ sudo apt-get remove docker docker-engine docker.io containerd runc
```

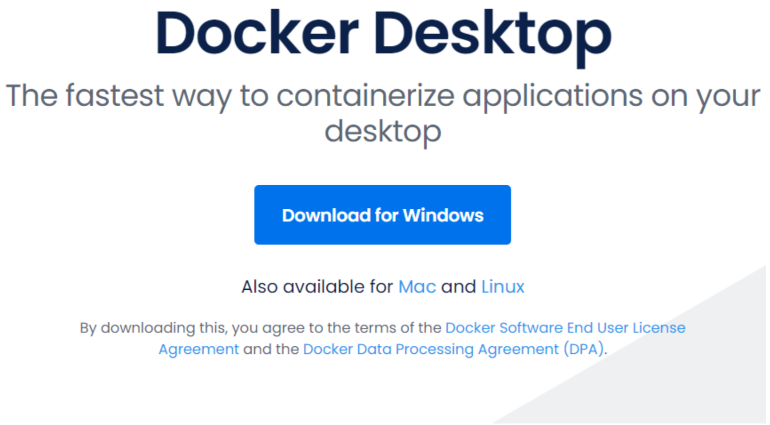
Source: docs.docker.com

https://www.docker.com › products › docker-desktop

Docker Desktop for Mac and Windows | Docker

Learn why **Docker** Desktop is the preferred choice for millions of developers building containerized applications. **Download** for Mac or Windows.

Step 2: After clicking the link, choose your OS, be it Windows, MAC, or Linux for installation.



Docker Desktop

The fastest way to containerize applications on your desktop

Also available for Mac and Linux

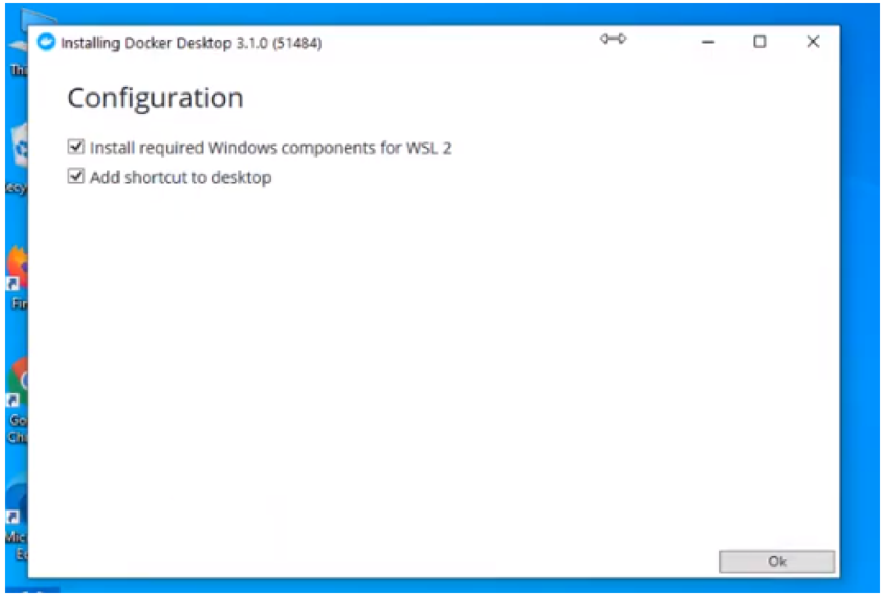
By downloading this, you agree to the terms of the Docker Software End User License Agreement and the Docker Data Processing Agreement (DPA).

Start Docker Desktop Tool

Step 3: After installation, it will look something like this in Windows:

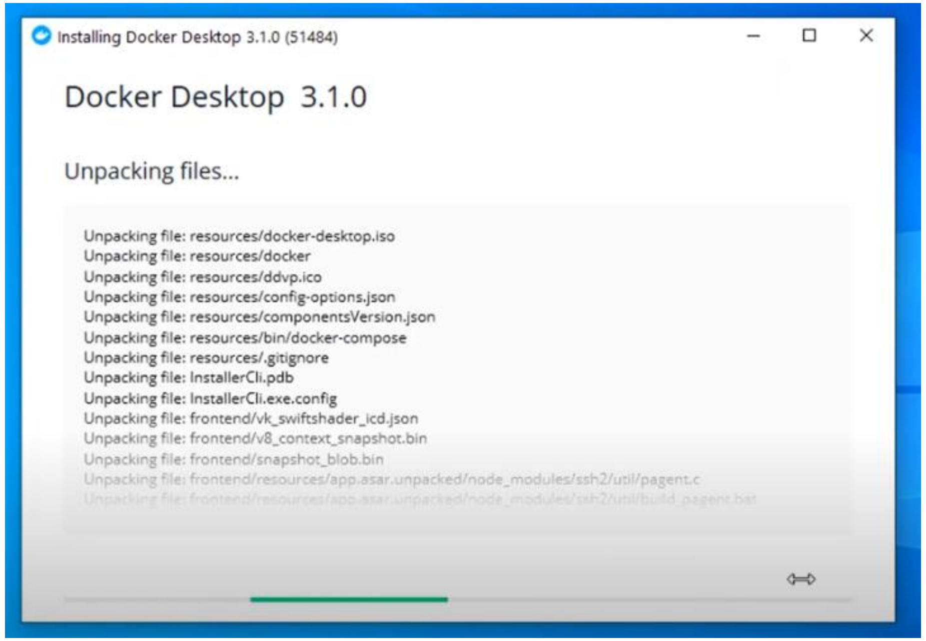
1) Open the Docker Desktop.
2) Accept the Docker Subscription Service Agreement window. and click On continue. Docker Desktop will start after we accept the terms and conditions.

Step 4: After clicking Ok the installation will start.


Installing Docker Desktop 3.1.0 (51484)

Configuration

☑ Install required Windows components for WSL 2
☑ Add shortcut to desktop

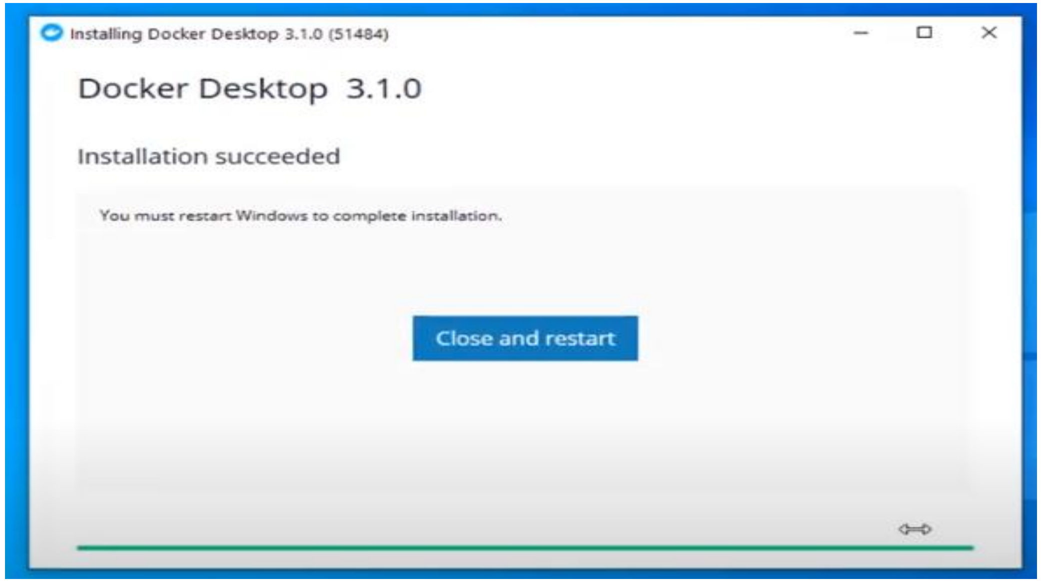

Installing Docker Desktop 3.1.0 (51484)

Docker Desktop 3.1.0

Unpacking files...

```
Unpacking file: resources/docker-desktop.iso
Unpacking file: resources/docker
Unpacking file: resources/ddvp.ico
Unpacking file: resources/config-options.json
Unpacking file: resources/componentsVersion.json
Unpacking file: resources/bin/docker-compose
Unpacking file: resources/.gitignore
Unpacking file: InstallerCli.pdb
Unpacking file: InstallerCli.exe.config
Unpacking file: frontend/vk_swiftshader_icd.json
Unpacking file: frontend/v8_context_snapshot.bin
Unpacking file: frontend/snapshot_blob.bin
Unpacking file: frontend/resources/app.asar.unpacked/node_modules/ssh2/util/pagent.c
Unpacking file: frontend/resources/app.asar.unpacked/node_modules/ssh2/util/build_pagent.bat
```

Step 5: After installation, it will show something like the below:



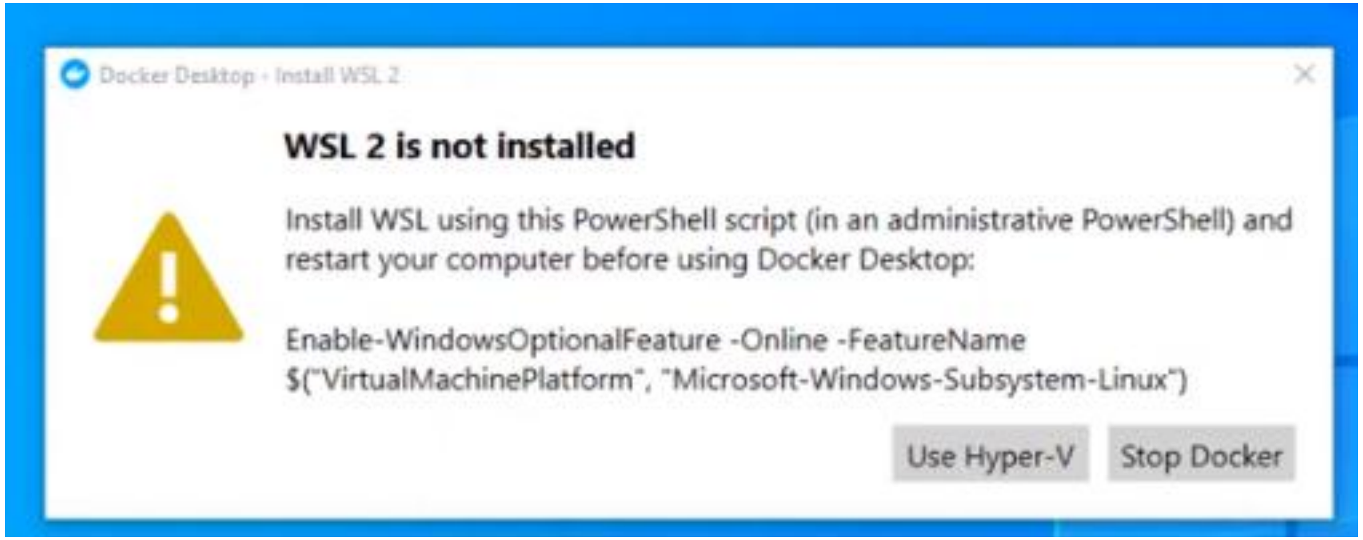
Installing Docker Desktop 3.1.0 (51484)

Docker Desktop 3.1.0

Installation succeeded

You must restart Windows to complete installation.

Step 6: After installation, we need to restart our PC and install WSL 2, which stands for Windows Setup for LINUX. It is a compatibility layer for running Linux binary executables natively on Windows 10. Please follow the next few instructions carefully. After restarting, the following dialog box will appear, then click on the Stop Docker button there.



Docker Desktop - Install WSL 2

WSL 2 is not installed

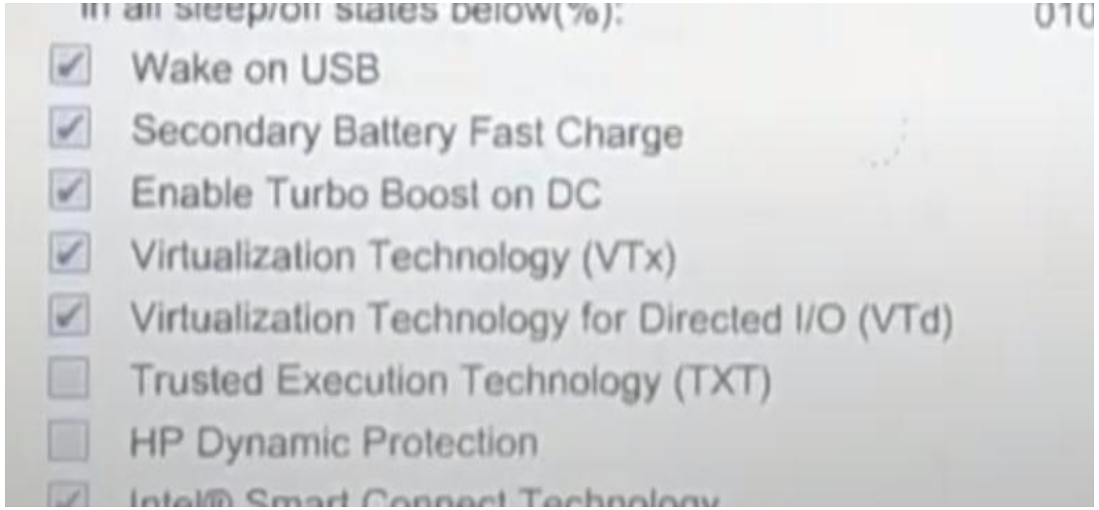
Install WSL using this PowerShell script (in an administrative PowerShell) and restart your computer before using Docker Desktop:

```
Enable-WindowsOptionalFeature -Online -FeatureName
$("VirtualMachinePlatform", "Microsoft-Windows-Subsystem-Linux")
```

Step 7: After clicking, we need to enable the Hyper-V, for that we will restart the PC and go to BIOS setup, Settings>Update and Security>Recovery>Advanced Setup>Device Configuration. After that, if the option Enable Turbo Boost on DC. is unmarked, mark it, after it, save, and exit.

Step 8: Afterward, in the last step, go to Control Panel> Turn Windows Features on and off. Then for activating Hyper-V, mark the Hyper-V and Windows Hypervisor Platform.

At this point, you have successfully installed and configured Docker on your Windows machine.



in all sleep/off states below(%): 010

☑ Wake on USB

☑ Secondary Battery Fast Charge

☑ Enable Turbo Boost on DC

☑ Virtualization Technology (VTx)

☑ Virtualization Technology for Directed I/O (VTd)

□ Trusted Execution Technology (TXT)

□ HP Dynamic Protection

☑ Intel® Smart Connect Technology

Applications of docker

1) **Software Development:** Developers use Docker to streamline the development process by creating isolated environments for building, testing, and deploying applications.
2) **Continuous Integration/Continuous Deployment (CI/CD):** Docker facilitates automated testing and deployment pipelines, allowing for rapid and efficient software delivery.
3) **Microservices Architecture:** Docker containers are ideal for implementing microservices, enabling modular and scalable application architectures.
4) **Cloud Computing:** Docker containers are widely used in cloud environments for resource-efficient deployment and scaling of applications.
5) **DevOps Practices:** Docker promotes collaboration between development and operations teams, fostering the adoption of DevOps practices.
6) **Big Data and Analytics:** Docker containers provide a consistent environment for running big data and analytics tools, simplifying deployment and management.

Serverless Lambda

- Serverless Lambda, often referred to as **AWS Lambda**,is a serverless computing service provided by Amazon Web Services (AWS).
- It allows developers **to run code without provisioning or managing servers.**
- With Serverless Lambda, **you can upload your code, specify the event sources** (such as HTTP requests or changes to data in storage services), and AWS will automatically execute your code in response to those events.

Steps for serverless lambda

Setup Serverless Framework

1) Open https://app.serverless.com/?view=register and sign up for serverless account which is free for basic development.

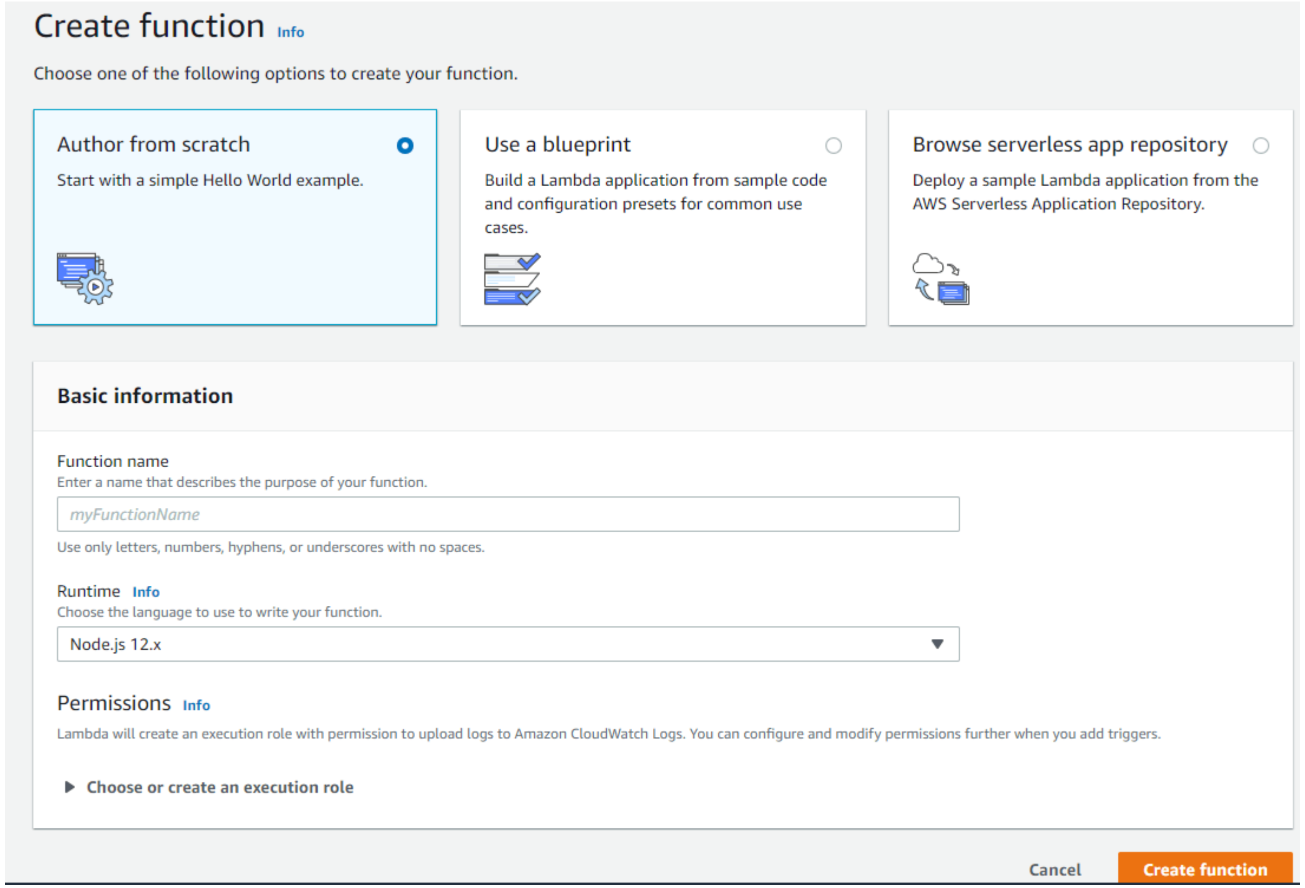
2) Open up terminal and type **npm install -g serverless** to install serverless

3) Once the installation process is complete you can verify serverless is installed by running the following command

serverless — version

Setting up AWS for serverless framework

1) First, login to AWS console at this URL: https://aws.amazon.com/console/. Click on Lambda under Compute or simply search Lambda in the services search field.
2) Now click the button labeled "Create function." You will get to the screen below where you enter a function name (firstFunction) and select Node JS 12. Then click Create at the bottom right of the screen.



Create function Info

Choose one of the following options to create your function.

Author from scratch ●
Start with a simple Hello World example.

Use a blueprint ○
Build a Lambda application from sample code and configuration presets for common use cases.

Browse serverless app repository ○
Deploy a sample Lambda application from the AWS Serverless Application Repository.

Basic information

Function name
Enter a name that describes the purpose of your function.
myFunctionName
Use only letters, numbers, hyphens, or underscores with no spaces.

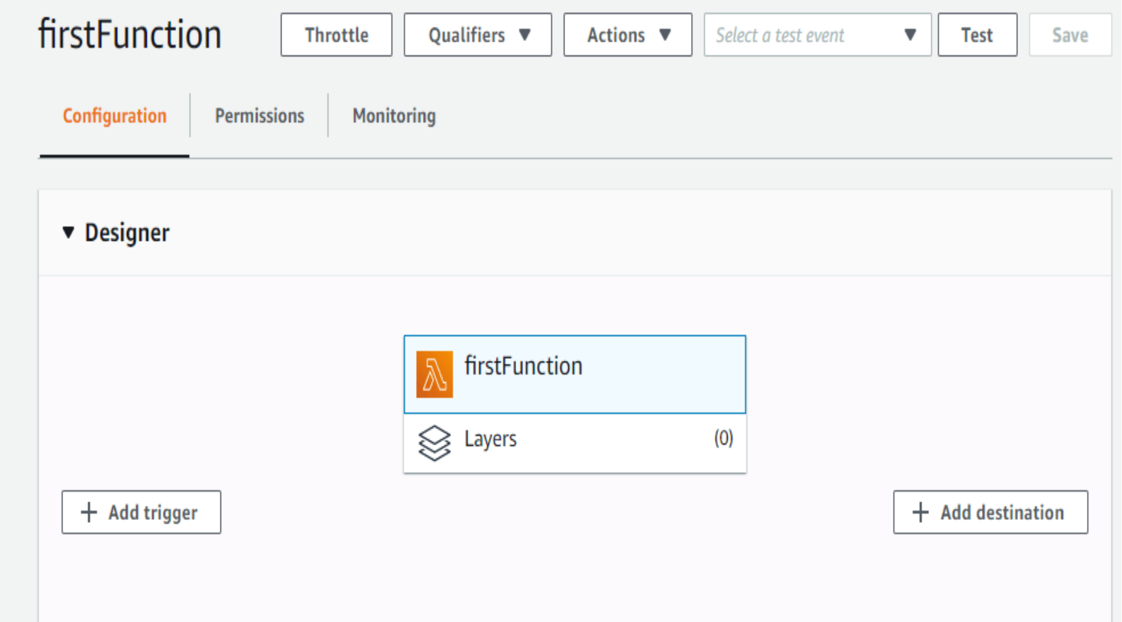
Runtime Info
Choose the language to use to write your function.
Node.js 12.x ▼

Permissions Info
Lambda will create an execution role with permission to upload logs to Amazon CloudWatch Logs. You can configure and modify permissions further when you add triggers.

▶ Choose or create an execution role

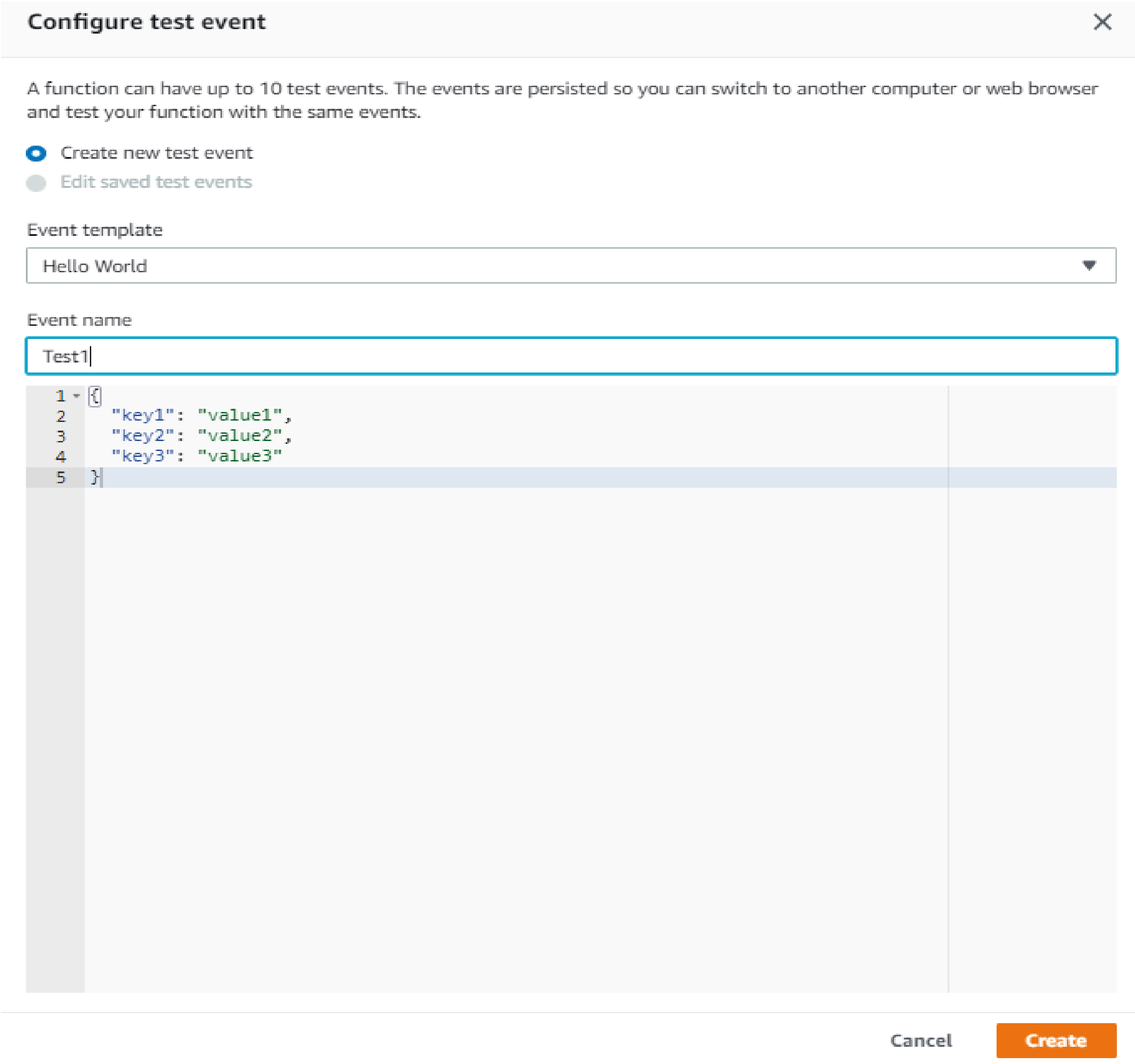
3) Choosing Node.js allows us to program the serverless function with JavaScript. I'm illustrating how to use functions with JavaScript as it is a very common language but feel free to use another language if you are more comfortable with it, everything we cover here apply to other languages.

You will get to the screen like this :



4) Scroll down to the source code and replace “Hello from Lambda” with “Hello from my first function.”

5) Click Save at to top right and then click Test. You will get to a screen to create a test event to be passed to your function. At this stage we are not using anything from the event so just enter an event name and click Create.



Configure test event

A function can have up to 10 test events. The events are persisted so you can switch to another computer or web browser and test your function with the same events.

● Create new test event
○ Edit saved test events

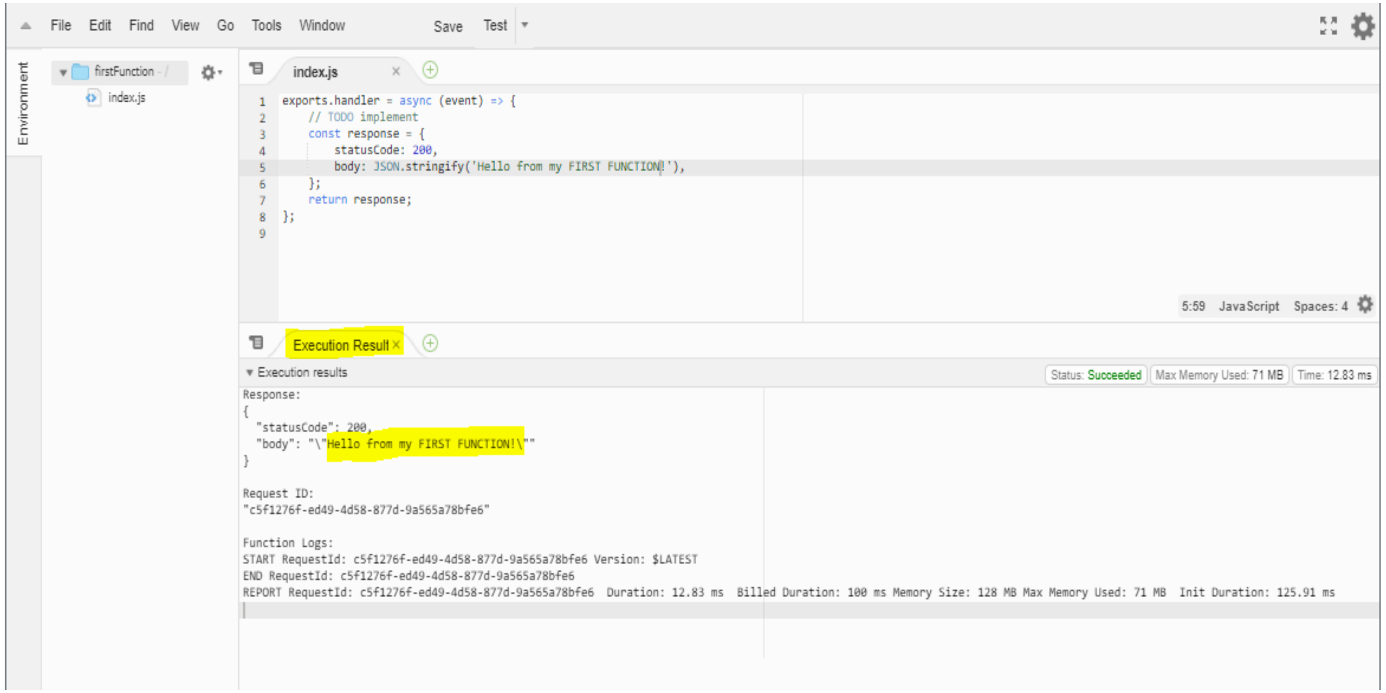
Event template: Hello World

Event name: Test1

```
{
  "key1": "value1",
  "key2": "value2",
  "key3": "value3"
}
```

6) Now you will be back to the editor screen, click Test again. That will run your function with the test event you just created. You will see a successful execution and its result will be displayed in a new tab called “Execution Result,” under the source code.

You will see the result of the execution as well as the unique request ID and the log.



```
exports.handler = async (event) => {
    // TODO implement
    const response = {
        statusCode: 200,
        body: JSON.stringify('Hello from my FIRST FUNCTION!'),
    };
    return response;
};
```

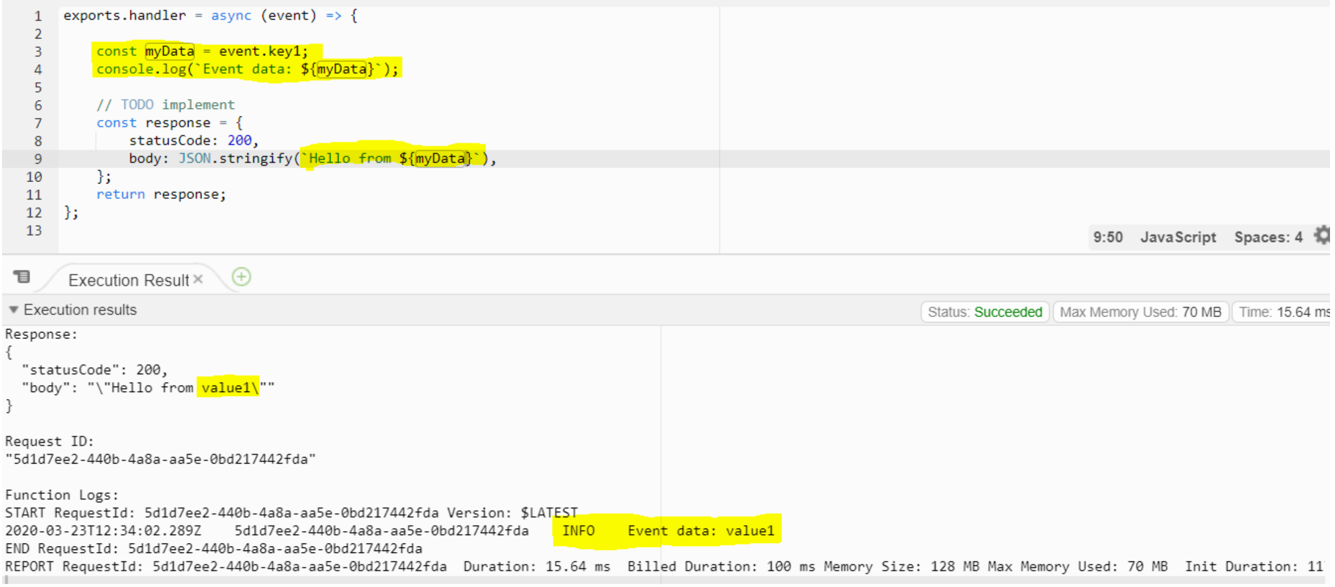
```
Response:
{
  "statusCode": 200,
  "body": "\"Hello from my FIRST FUNCTION!\""
}

Request ID:
"c5f1276f-ed49-4d58-877d-9a565a78bfe6"

Function Logs:
START RequestId: c5f1276f-ed49-4d58-877d-9a565a78bfe6 Version: $LATEST
END RequestId: c5f1276f-ed49-4d58-877d-9a565a78bfe6
REPORT RequestId: c5f1276f-ed49-4d58-877d-9a565a78bfe6  Duration: 12.83 ms  Billed Duration: 100 ms Memory Size: 128 MB Max Memory Used: 71 MB  Init Duration: 125.91 ms
```

Now let's see how we pass data to the function:

7) Change the code as highlighted below and rerun the test:



```
exports.handler = async (event) => {

    const myData = event.key1;
    console.log(`Event data: ${myData}`);

    // TODO implement
    const response = {
        statusCode: 200,
        body: JSON.stringify(`Hello from ${myData}`),
    };
    return response;
};

```

```
Response:
{
  "statusCode": 200,
  "body": "\"Hello from value1\""
}

Request ID:
"5d1d7ee2-440b-4a8a-aa5e-0bd217442fda"

Function Logs:
START RequestId: 5d1d7ee2-440b-4a8a-aa5e-0bd217442fda Version: $LATEST
2020-03-23T12:34:02.289Z    5d1d7ee2-440b-4a8a-aa5e-0bd217442fda    INFO    Event data: value1
END RequestId: 5d1d7ee2-440b-4a8a-aa5e-0bd217442fda
REPORT RequestId: 5d1d7ee2-440b-4a8a-aa5e-0bd217442fda  Duration: 15.64 ms  Billed Duration: 100 ms Memory Size: 128 MB Max Memory Used: 70 MB  Init Duration: 11
```

Benefits of Serverless lambda

1) **No need for managing servers :** Run code without provisioning or managing infrastructure. Simply write and upload code as a .zip file or container image.
2) **Automatic scaling :** Automatically respond to code execution requests at any scale, from a dozen events per day to hundreds of thousands per second.
3) **Pay-as-you-go pricing :** Save costs by paying only for the compute time you use—by the millisecond—instead of provisioning infrastructure upfront for peak capacity.
4) **Performance optimization :** Optimize code execution time and performance with the right function memory size. Respond to high demand in double-digit milliseconds with Provisioned Concurrency.

Use Cases of Serverless Lambda

1) **Web Applications:** AWS Lambda can be used to build serverless web applications, where functions are triggered by HTTP requests. This allows developers to create dynamic and scalable web applications without managing servers.

2) **Real-time Data Processing :** Lambda functions can be triggered by events from various AWS services such as S3, DynamoDB, Kinesis, or IoT. This enables real-time data processing, analytics, and event-driven architectures.

3) **Mobile and IoT Applications:** Lambda functions can be integrated with mobile and IoT applications to handle backend logic, process data from sensors, and respond to user actions in real-time.

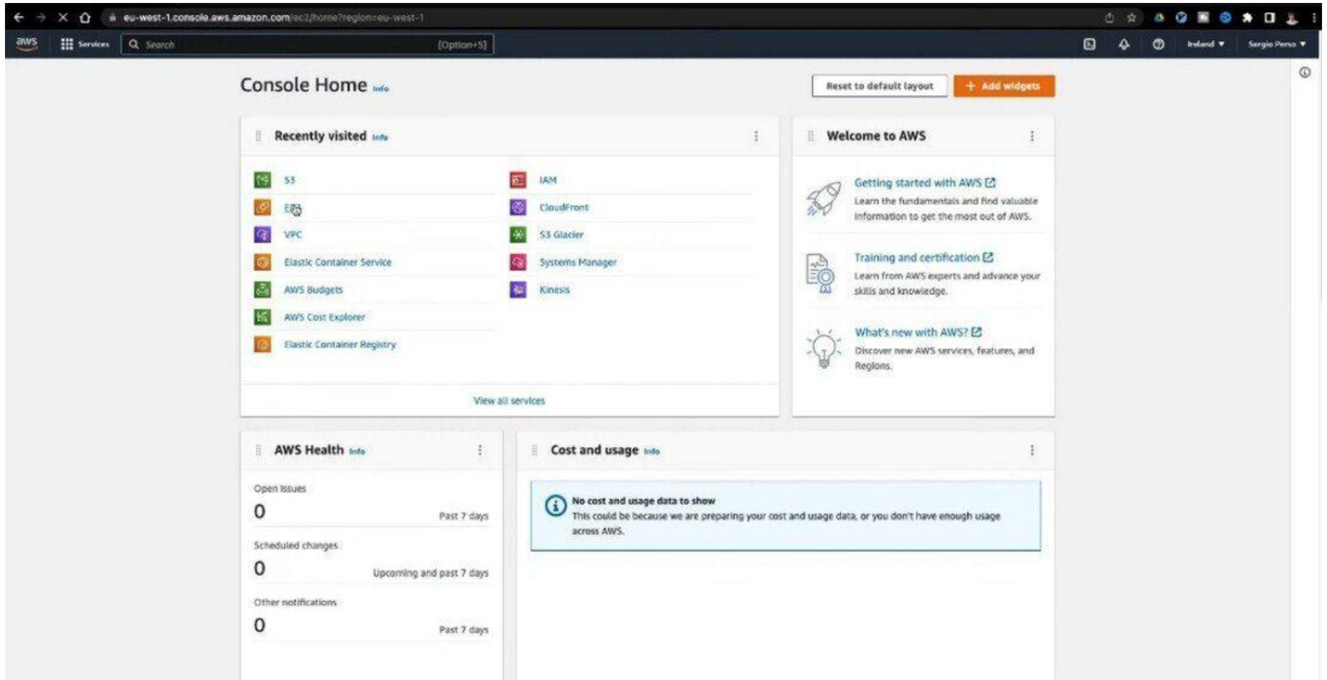
4) **Image and Media Processing:** Lambda functions can be used for image resizing, video transcoding, and other media processing tasks. They can be triggered by file uploads to S3 buckets or other storage services.

Microservices

- Microservices are an architectural and organizational approach to software development where software is composed of small independent services that communicate over well-defined APIs.
- Microservices architectures make applications easier to scale and faster to develop, enabling innovation and accelerating time-to-market for new features.
- Microservices are Autonomous and Specialized.
- In the context of AWS (Amazon Web Services), microservices can be implemented using various AWS services and tools.

How to Deploy a Microservices Architecture with AWS?

Step 1: Load Balancer and Target Group.Navigate to the AWS Management Console and go to EC2.



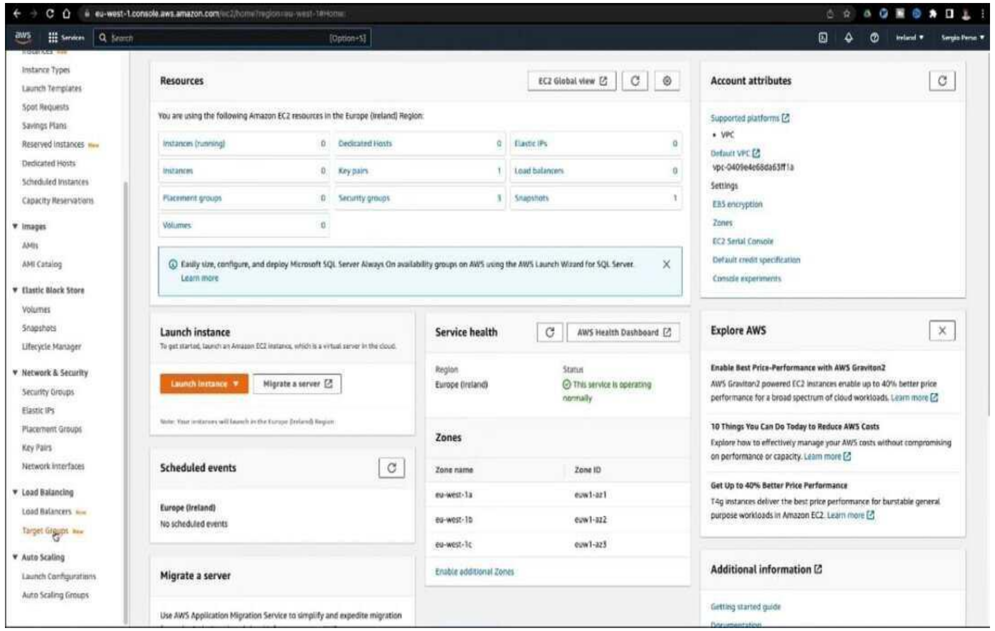
Learn the fundamentals and find valuable information to get the most out of AWS.

Learn from AWS experts and advance your skills and knowledge.

Discover new AWS services, features, and Regions.

No cost and usage data to show
This could be because we are preparing your cost and usage data, or you don't have enough usage across AWS.

Step 2: Click on Load Balancers and create a new Application Load Balancer. Create a new target group associated with your load balancer.Define target group targets (ECS instances) and health checks.



Resources

You are using the following Amazon EC2 resources in the Europe (Ireland) Region:

Instances (running)	0	Dedicated Hosts	0	Elastic IPs	0
Instances	0	Key pairs	1	Load balancers	0
Placement groups	0	Security groups	3	Snapshots	1
Volumes	0				

Easily size, configure, and deploy Microsoft SQL Server Always On availability groups on AWS using the AWS Launch Wizard for SQL Server. Learn more

Account attributes

Supported platforms
- VPC

Default VPC
vpc-0409e4e68da63ff1a

Settings

EBS encryption

Zones

EC2 Serial Console

Default credit specification

Console experiments

Launch instance

To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.

Note: Your instances will launch in the Europe (Ireland) Region

Service health

Region: Europe (Ireland)

Status: This service is operating normally

Zones

Zone name	Zone ID
eu-west-1a	euw1-az1
eu-west-1b	euw1-az2
eu-west-1c	euw1-az3

Enable additional Zones

Scheduled events

Europe (Ireland)

No scheduled events

Migrate a server

Use AWS Application Migration Service to simplify and expedite migration

Explore AWS

Enable Best Price-Performance with AWS Graviton2

AWS Graviton2 powered EC2 instances enable up to 40% better price performance for a broad spectrum of cloud workloads. Learn more

10 Things You Can Do Today to Reduce AWS Costs

Explore how to effectively manage your AWS costs without compromising on performance or capacity. Learn more

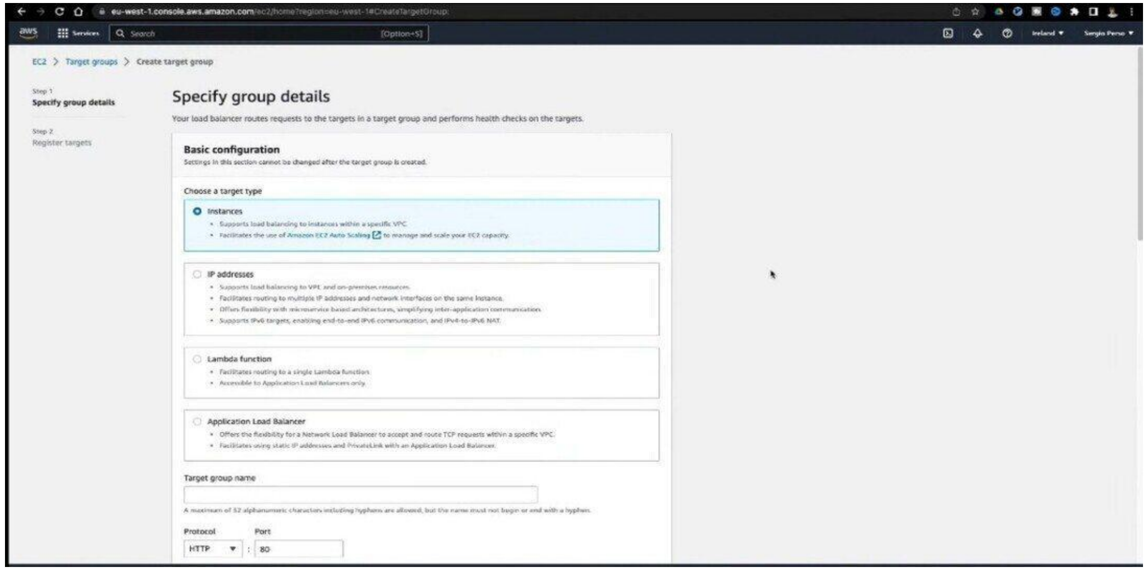
Get Up to 40% Better Price Performance

T4g instances deliver the best price performance for burstable general purpose workloads in Amazon EC2. Learn more

Additional information

Getting started guide

Documentation


eu-west-1.console.aws.amazon.com/ec2/home?region=eu-west-1#CreateTargetGroup:
Services
Search
[Option+S]
Ireland ▼
Sergio Perso ▼
EC2 > Target groups > Create target group
Step 1
Specify group details
Step 2
Register targets

Specify group details

Your load balancer routes requests to the targets in a target group and performs health checks on the targets.

Basic configuration

Settings in this section cannot be changed after the target group is created.

Choose a target type

● Instances
- Supports load balancing to instances within a specific VPC.
- Facilitates the use of Amazon EC2 Auto Scaling to manage and scale your EC2 capacity.

○ IP addresses
- Supports load balancing to VPC and on-premises resources.
- Facilitates routing to multiple IP addresses and network interfaces on the same instance.
- Offers flexibility with microservice based architectures, simplifying inter-application communication.
- Supports IPv6 targets, enabling end-to-end IPv6 communication, and IPv4-to-IPv6 NAT.

○ Lambda function
- Facilitates routing to a single Lambda function.
- Accessible to Application Load Balancers only.

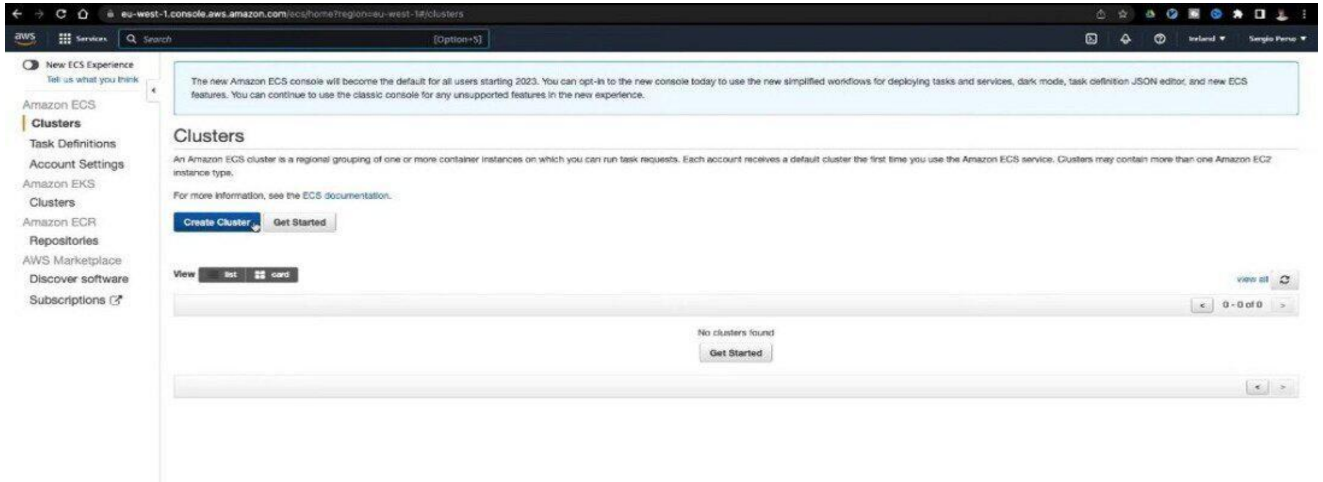
○ Application Load Balancer
- Offers the flexibility for a Network Load Balancer to accept and route TCP requests within a specific VPC.
- Facilitates using static IP addresses and PrivateLink with an Application Load Balancer.

Target group name

A maximum of 32 alphanumeric characters including hyphens are allowed, but the name must not begin or end with a hyphen.

Protocol: HTTP ▼ : Port: 80

Step 3: Create ECS Cluster.In the AWS Management Console, go to ECS.Create a new ECS cluster.



The new Amazon ECS console will become the default for all users starting 2023. You can opt-in to the new console today to use the new simplified workflows for deploying tasks and services, dark mode, task definition JSON editor, and new ECS features. You can continue to use the classic console for any unsupported features in the new experience.

Clusters

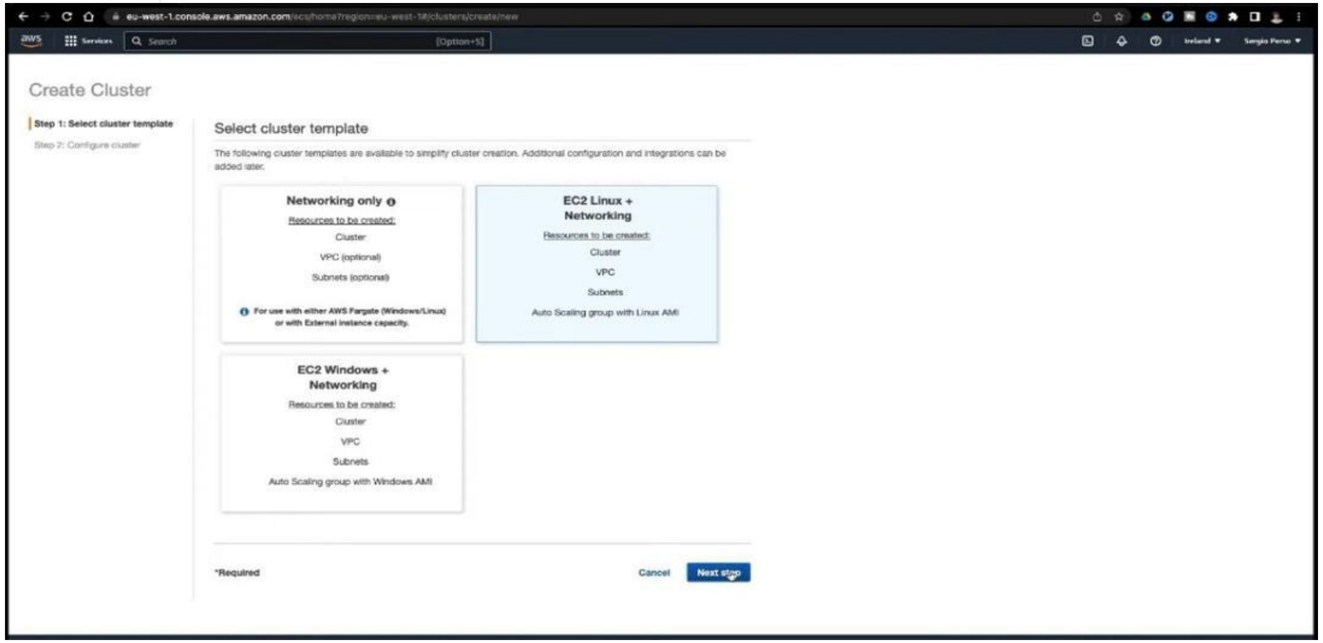
An Amazon ECS cluster is a regional grouping of one or more container instances on which you can run task requests. Each account receives a default cluster the first time you use the Amazon ECS service. Clusters may contain more than one Amazon EC2 instance type.

For more information, see the ECS documentation.

No clusters found

Step 5: Choose networking options and click on next

configure your cluster give name to your cluster


eu-west-1.console.aws.amazon.com/ecs/home?region=eu-west-1#/clusters/create/new
aws
Services
Search
[Option+S]
Ireland ▼
Sergio Perso ▼
Step 1: Select cluster template
Step 2: Configure cluster
Cancel
Next step

Create Cluster

Select cluster template

The following cluster templates are available to simplify cluster creation. Additional configuration and integrations can be added later.

Networking only
Resources to be created:
Cluster
VPC (optional)
Subnets (optional)
For use with either AWS Fargate (Windows/Linux) or with External instance capacity.

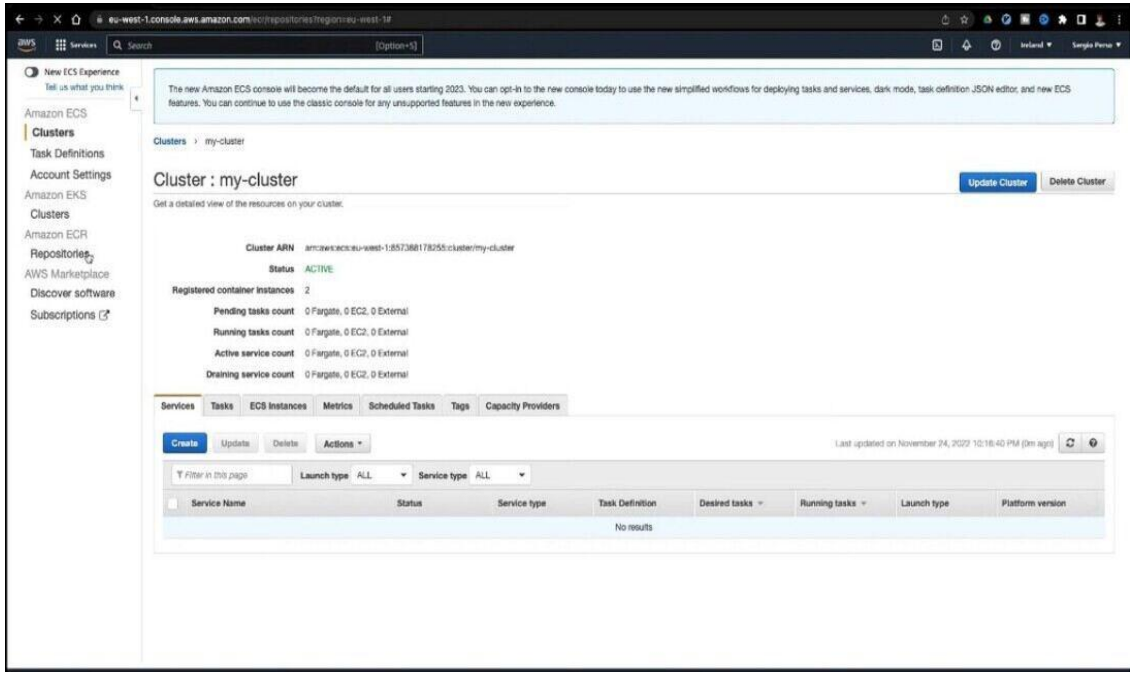
EC2 Linux + Networking
Resources to be created:
Cluster
VPC
Subnets
Auto Scaling group with Linux AMI

EC2 Windows + Networking
Resources to be created:
Cluster
VPC
Subnets
Auto Scaling group with Windows AMI

*Required

Create ECS Task. Click on the repository

configure your repository , make sure it is private.



The new Amazon ECS console will become the default for all users starting 2023. You can opt-in to the new console today to use the new simplified workflows for deploying tasks and services, dark mode, task definition JSON editor, and new ECS features. You can continue to use the classic console for any unsupported features in the new experience.

Clusters › my-cluster

Cluster : my-cluster

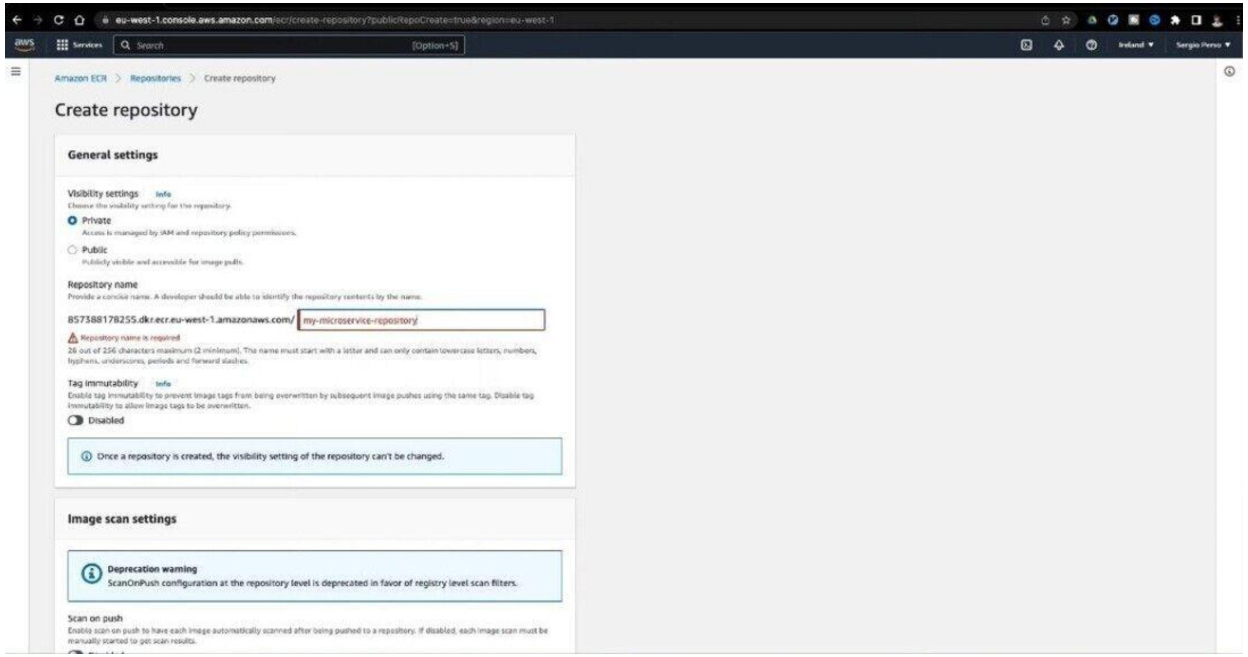
Get a detailed view of the resources on your cluster.

Cluster ARN	arn:aws:ecs:eu-west-1:857388178255:cluster/my-cluster
Status	ACTIVE
Registered container instances	2
Pending tasks count	0 Fargate, 0 EC2, 0 External
Running tasks count	0 Fargate, 0 EC2, 0 External
Active service count	0 Fargate, 0 EC2, 0 External
Draining service count	0 Fargate, 0 EC2, 0 External

Last updated on November 24, 2022 10:16:40 PM (0m ago)

Filter in this page Launch type ALL ▾ Service type ALL ▾

Service Name	Status	Service type	Task Definition	Desired tasks	Running tasks	Launch type	Platform version
No results							


eu-west-1.console.aws.amazon.com/ecr/create-repository?publicRepoCreate=true&region=eu-west-1
Services
Search
[Option+S]
Ireland ▾
Sergio Perso ▾

Amazon ECR > Repositories > Create repository

Create repository

General settings

Visibility settings Info

Choose the visibility setting for the repository.

● Private

Access is managed by IAM and repository policy permissions.

○ Public

Publicly visible and accessible for image pulls.

Repository name

Provide a concise name. A developer should be able to identify the repository contents by the name.

857388178255.dkr.ecr.eu-west-1.amazonaws.com/ my-microservice-repository

Repository name is required

26 out of 256 characters maximum (2 minimum). The name must start with a letter and can only contain lowercase letters, numbers, hyphens, underscores, periods and forward slashes.

Tag immutability Info

Enable tag immutability to prevent image tags from being overwritten by subsequent image pushes using the same tag. Disable tag immutability to allow image tags to be overwritten.

Disabled

Once a repository is created, the visibility setting of the repository can't be changed.

Image scan settings

Deprecation warning

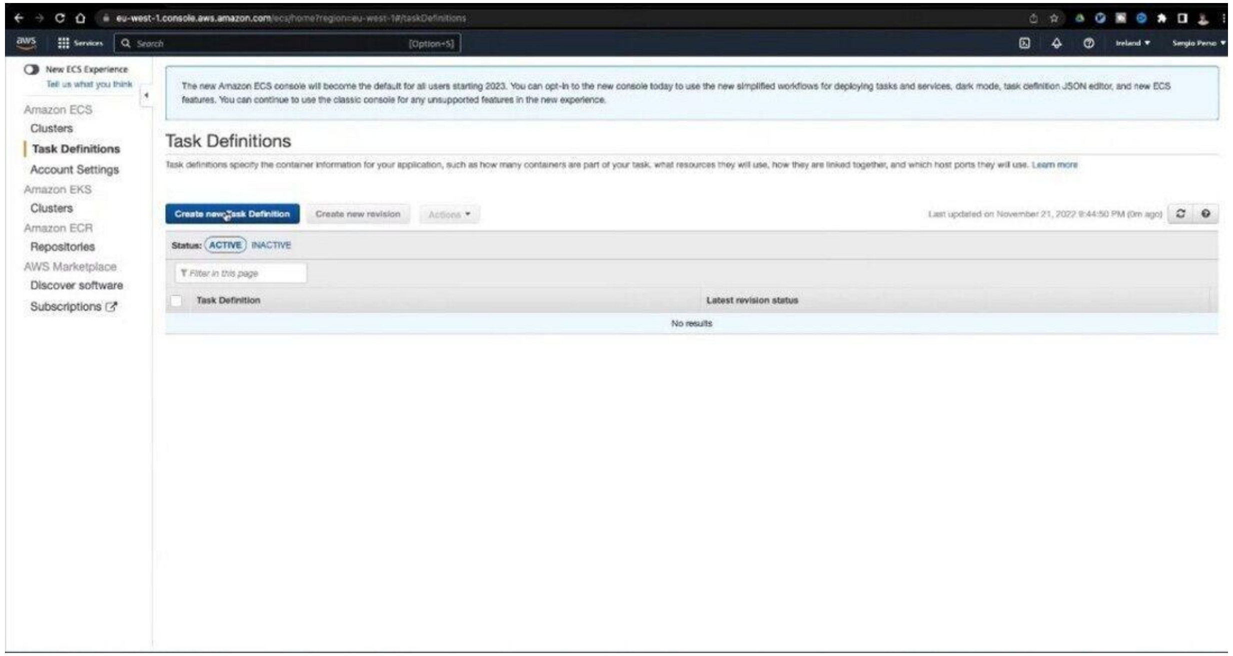
ScanOnPush configuration at the repository level is deprecated in favor of registry level scan filters.

Scan on push

Enable scan on push to have each image automatically scanned after being pushed to a repository. If disabled, each image scan must be manually started to get scan results.

Create Task Definitions

Define undertaking definitions for your microservices, specifying Docker snapshots, ports, environment variables, and useful resource requirements.



The new Amazon ECS console will become the default for all users starting 2023. You can opt-in to the new console today to use the new simplified workflows for deploying tasks and services, dark mode, task definition JSON editor, and new ECS features. You can continue to use the classic console for any unsupported features in the new experience.

Task Definitions

Task definitions specify the container information for your application, such as how many containers are part of your task, what resources they will use, how they are linked together, and which host ports they will use. Learn more

Last updated on November 21, 2022 9:44:50 PM (0m ago)

Task Definition	Latest revision status
No results	

Step 4: Update ECS Task

Update Task Definitions: If you need to make changes to your microservices (e.g., replace environment variables, exchange field configurations), adjust the project definitions.Update ECS Service: Update your ECS provider to use the updated undertaking definitions.

Benefits of Microservices

1) **Agility :** Microservices foster an organization of small, independent teams that take ownership of their services. Teams act within a small and well understood context, and are empowered to work more independently and more quickly. This shortens development cycle times. You benefit significantly from the aggregate throughput of the organization.

2) **Flexible Scaling :** Microservices allow each service to be independently scaled to meet demand for the application feature it supports. This enables teams to right-size infrastructure needs, accurately measure the cost of a feature, and maintain availability if a service experiences a spike in demand.

3) **Easy Deployment :** Microservices enable continuous integration and continuous delivery, making it easy to try out new ideas and to roll back if something doesn’t work. The low cost of failure enables experimentation, makes it easier to update code, and accelerates time-to-market for new features.

4) **Technological Freedom :** Microservices architectures don’t follow a “one size fits all” approach. Teams have the freedom to choose the best tool to solve their specific problems. As a consequence, teams building microservices can choose the best tool for each job.

How do Microservices work?

Microservices work by breaking down an application into a collection of smaller services that are each able to be developed, deployed, and scaled independently.

- Each service is self-contained and should implement a single business capability.
- Services communicate with each other through APIs and can be updated independently of the rest of the application.

Microservices Example

Consider an e-commerce application. Instead of having a single, monolithic application, the application could be broken down into several microservices.

- One microservice might handle user authentication, another might handle product catalog management, and a third might handle order processing.
- Each of these microservices could be developed and deployed independently, allowing the e-commerce application to scale and evolve more flexibly.

Cloud Forensics

- Cloud forensics refers to the use of forensic techniques to investigate cloud environments.
- When unlawful or criminal behavior has occurred using the cloud as a medium, cloud forensics experts use their skills and knowledge to detect the individuals or groups responsible.
- Cloud forensics encompasses users of the cloud, both victims and perpetrators.
- For example, a company using cloud servers might be the victim of a data breach or denial of the service incident. Criminals themselves might also use the cloud to launch an attack.

How Cloud Forensics Impacts User Security, Privacy?

- **Investigation and Analysis:** Cloud forensics allows for thorough investigation and analysis of security incidents, including unauthorized access, data breaches, and insider threats in cloud environments.
- **Data Recovery and Reconstruction:** Forensic techniques enable the recovery and reconstruction of lost or deleted data from cloud storage and computing resources, ensuring the integrity and availability of critical information.
- **Privacy Protection and Compliance:** Cloud forensics helps organizations ensure compliance with data protection regulations and privacy laws by detecting and addressing violations of user privacy rights, such as unauthorized access to sensitive data and data leakage incidents.

Tools and techniques of cloud forensics

1) **Log Analysis Tools:** Tools like Splunk, ELK Stack (Elasticsearch, Logstash, Kibana), and Sumo Logic are used to analyze logs from various cloud services to identify security incidents and anomalies.
2) **Forensic Imaging Tools:** Tools such as FTK Imager and dd (command-line tool) are used to create forensic images of cloud storage volumes or instances for investigation purposes.
3) **Network Traffic Analysis Tools:** Tools like Wireshark and CloudShark are used to capture and analyze network traffic between cloud services and endpoints to detect suspicious activities or unauthorized access.
4) **Memory Forensics Tools:** Tools like Volatility and Rekall are used to perform memory forensics on cloud instances to identify malware, unauthorized processes, or security breaches.
5) **Cloud-specific Forensic Tools:** Some cloud providers offer their own forensic tools and services tailored to their platforms, such as AWS CloudTrail for auditing and AWS GuardDuty for threat detection.

References

1) https://www.studocu.com/in/document/jain-deemed-to-be-university/cloud-computing/elicit-the-pros-and-cons-of-content-level-security/47953912
2) https://docs.docker.com/get-started/overview/
3) https://aws.amazon.com/lambda/
4) https://www.geeksforgeeks.org/introduction-to-aws-lambda/
5) https://aws.amazon.com/microservices/
6) https://www.geeksforgeeks.org/microservices/
7) https://www.eccouncil.org/cybersecurity-exchange/computer-forensics/what-is-cloud-forensics/
8) https://www.appdirect.com/blog/cloud-forensics-and-the-digital-crime-scene

Learning Resources

Text books

1. Rajkumar Buyya, Christian Vecchiola, S. Thamarai Selvi, “Mastering Cloud Computing”, Tata McGraw Hill, ISBN-13: 978-1-25-02995-0
2. Tim Mather, Subra K, Shahid L, Cloud Security and Privacy, OReilly, ISBN-13 978-81-8404-815-5
3. Rajkumar Buyya, James Broberg, Andrzej Goscinski, “Cloud computing Principles and Paradigms”, Wiley Publication.
4. Barrie Sosinsky, “Cloud Computing", Wiley India, ISBN: 978-0-470-90356-8
5. Kailash Jayaswal, “Cloud computing", Black Book, Dreamtech Press
6. Thomas Erl, Zaigham Mahmood and Ricardo Puttini, “Cloud Computing: Concepts, Technology and Architecture”, Pearson, 1st Edition.

Reference Books

1. Introduction to the Theory of Computation, Michael Sipser.
2. Introduction to Languages and the Theory of Computation, John Martin.
3. Computers and Intractability: A Guide to the Theory of NP Completeness, M. R. Garey and D. S. Johnson

Supplementary Reading:

1. Dr. Kumar Saurabh, “Cloud Computing”, Wiley Publication

Learning Resources

Web Resources:

i. https://www.ibm.com/cloud-computing/files/cloud-for-dummies.pdf

Web links

i. https://docs.aws.amazon.com/

ii. https://docs.microsoft.com/en-us/azure/

MOOCs:

i. https://www.coursera.org/learn/gcp-fundamentals
ii. https://nptel.ac.in/courses/106105167/

THANK YOU FOR LISTENING

ANY QUESTION ?