**Project Title:**

**Automated Deployment of EC2 Instances with Restricted Access using AWS CloudFormation (Infrastructure as Code)**

**Goal of the Project**

The main goal of this project is to **automate the creation and configuration of EC2 instances and IAM users** using AWS CloudFormation. Each IAM user is given access to **only their specific EC2 Windows instance**, and the entire infrastructure setup is done through a single CloudFormation template (YAML file).

The project ensures:

* Secure and restricted access to each EC2 instance.
* Use of individual key pairs for each user.
* Automation of infrastructure without manually provisioning resources.

**Main Use of AWS CloudFormation (IaC) in This Project**

Using CloudFormation as **Infrastructure as Code (IaC)** provides the following benefits over manual provisioning:

**🔹 Automation**

Instead of manually creating EC2 instances, IAM users, and policies through the AWS Console, everything is **automated using a CloudFormation YAML file**.

**🔹 Consistency & Reusability**

Every time the stack is launched, the resources are created **exactly the same way**, ensuring **consistent infrastructure**.

**🔹 Version Control**

The YAML template can be stored in Git or other version control systems, so **infrastructure changes are tracked** just like code.

**🔹 Faster Deployment**

Once the template is ready, the infrastructure can be **deployed within minutes**, saving time and effort.

**🔹 Error Reduction**

Manual steps are prone to errors. IaC reduces human error by automating everything.

**Steps a User Performs to Get His/Her Instance**

Each user follows these steps to access and manage their instance:

1. **Login to AWS Console** using the IAM credentials provided (username & password).
2. Navigate to the **EC2 Dashboard**.
3. View and manage only **their assigned EC2 instance** (Start/Stop/Restart/Get RDP password).
4. Use **their unique Key Pair** (e.g., suryaKeyPair, vikramKeyPair, chaithuKeyPair) to access the Windows instance via RDP (Remote Desktop).
5. No access to other users' instances or sensitive resources.

**Real-World Usage of This Project in IT Companies**

In real-world IT companies (such as Wipro, Infosys, Accenture, etc.), this approach is commonly used for:

**🔹 Internal Teams**

Dev, Test, QA, and Support teams are provided with **separate VMs**, often on the cloud, with access restrictions based on role and department.

**🔹 Client Projects**

For secure development and testing, **project-specific VMs are provided to team members**. Each member has access to only their assigned resources.

**🔹 Remote Working**

With the rise of remote work, employees log in to cloud-hosted machines. Key pairs and IAM roles restrict access and enhance security.

**🔹 Training and Labs**

For internal training, separate instances are created automatically using CloudFormation, with access isolated to each trainee.

**Conclusion**

This project showcases a practical and secure approach to managing user-specific cloud resources using AWS CloudFormation. It eliminates the need for manual setup, improves security, and aligns with real-world enterprise practices for efficient cloud resource management.