

1. What is SaaS?

A method of distributing programmes via the Internet as a service is known as software as a service (or SaaS). You may avoid complicated software and hardware maintenance by just accessing software via the Internet rather than installing and maintaining it.

SaaS applications are sometimes referred to as hosted software, web-based software, and on-demand software. Whatever name they go by, SaaS apps run on the servers of a SaaS provider. Security, availability, and performance of access to the application are all managed by the supplier.

Low setup and infrastructure costs

You just pay for what you need with no capital expenditure that needs to be depreciated on your balance sheet over time.

Accessible from anywhere

Just connect to the internet and you can work from wherever you need to be via desktop, laptop, tablet or mobile or other networked device.

Scalability

You can adapt your requirements to the number of people who need to use the system, the volume of data and the functionality required as your business grows.

Industry leading service level agreements (SLAs) for uptime and performance

So you have assurances that the software will be available to use when you need it – a difficult promise for in-house teams to make.

Automatic, frequent updates

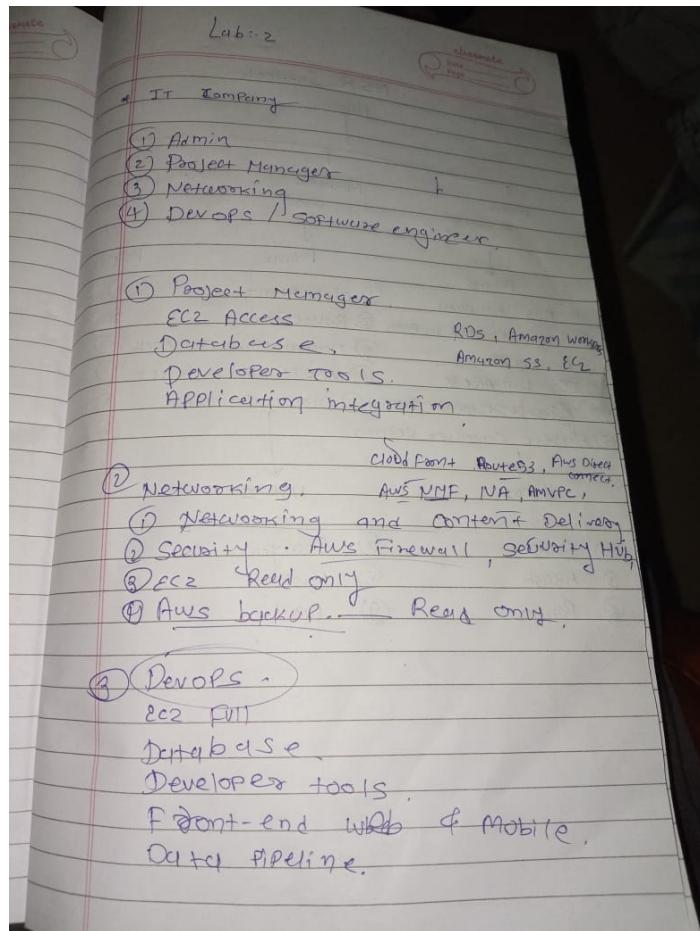
Providers offer timely improvements thanks to their scale and because they receive feedback about what their customers need. This frees up your IT department for other more business-critical tasks.

Security at the highest level required by any customer

Because of the shared nature of the service, all users benefit from the security level that's been set up for those with the highest need.

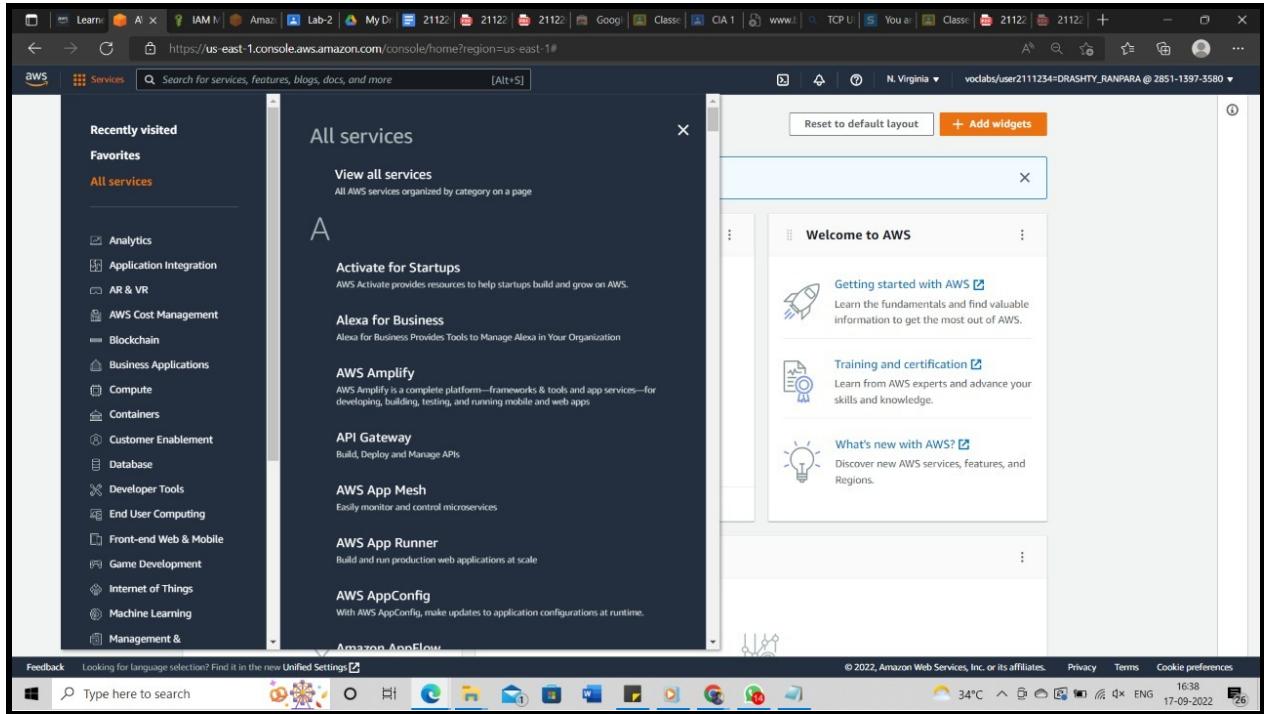
2. Create a project which has 3 different modules.

3. Identify the services required to run the modules (minimum 4 services for each modules)

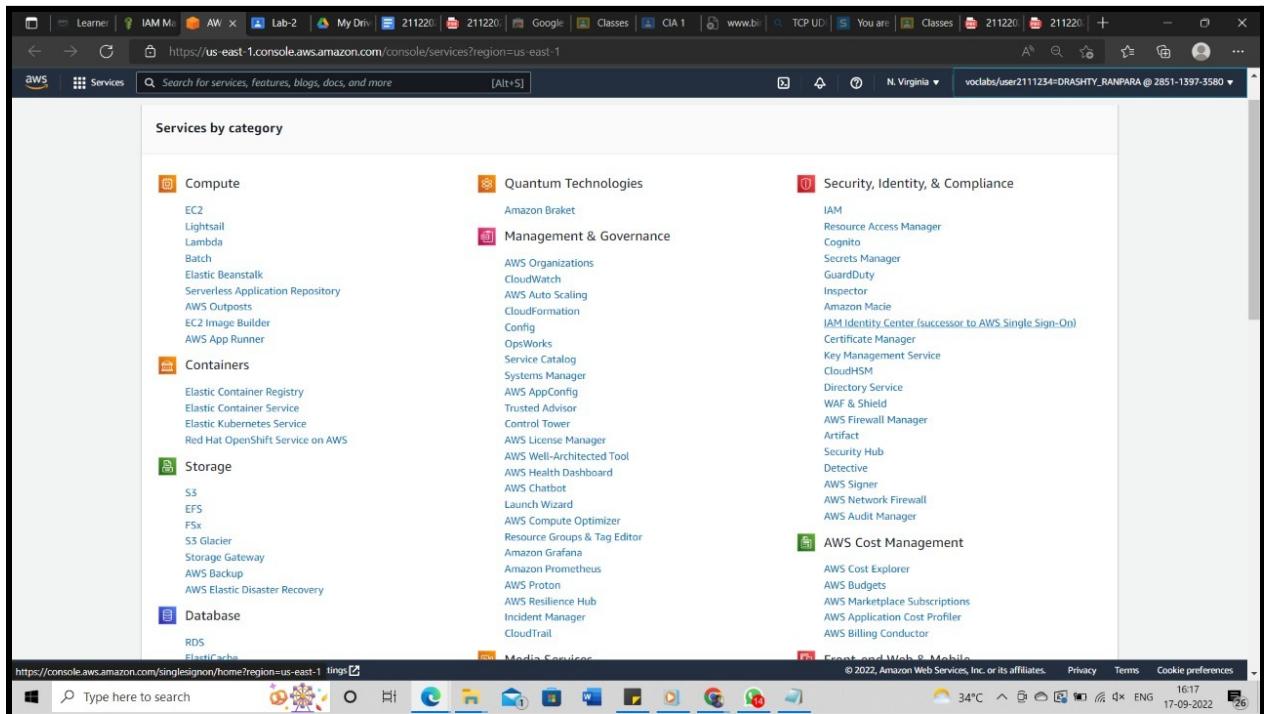


4. Identify the services required to run the modules (minimum 4 services for each modules)

Login to AWS Portal. Go to the Learner Lab program and click on the start lab button. It should show a green signal beside the AWS link. Navigate to Dashboard and click on services and in that click the all services and in that View All services.



All service will be displayed



Our Domain is IT infrastructure so there is the main Administrator and other three groups like Networking group, project manager Group and DevOPs Group. So creating the Group we move to the Dashboard which is under the Identity and access management.

The screenshot shows the AWS Identity and Access Management (IAM) dashboard. On the left, there's a navigation menu with sections like 'Access management' (User groups, Roles, Policies, Identity providers, Account settings), 'Access reports' (Access analyzer, Archive rules, Analyzers, Settings, Credential report, Organization activity, Service control policies (SCPs)), and 'Related consoles' (IAM Identity Center). The main area displays 'IAM resources' with counts: User groups (0), Users (0), Roles (14), Policies (4), and Identity providers (0). It also features 'Security recommendations' (Add MFA for root user), 'What's new' (updates for features in IAM), and a 'Tools' section with links to Policy simulator, Web identity federation playground, and IAM documentation. The top bar includes the AWS logo, search bar, and global navigation.

So on left panel we see the different items in the menu bar so from that menu bar select the User Group and click on the Create group button

The screenshot shows the 'User groups' page under the 'Access management' section. The left sidebar has the same structure as the previous dashboard. The main area shows a table with one row: 'User groups (0)'. A 'Create group' button is visible at the top right of the table. The bottom of the screen shows the Windows taskbar with various pinned icons and system status.

Add the name of the group

The screenshot shows the AWS IAM Management Console with the 'Create user group' page open. The 'User group name' field contains 'DevOps'. Below it, there's a section for 'Add users to the group - Optional' and another for 'Attach permissions policies - Optional'. The browser status bar shows the URL https://us-east-1.console.aws.amazon.com/iamv2/home?region=us-east-1#/groups/create.

After that, Apply the policies of the groups. Here I am making DevOPs Group and other members create Networking as well as Project Manager.

5. Identify the services required to run the modules (minimum 4 services for each modules)

Applying the policies

In DevOPs Group there is policies

1. CodePipeline Full Access
2. DataPipeline Full Access

The screenshot shows the 'Attach permissions policies' section in the AWS IAM Management Console. A search bar at the top shows 'pipeline'. Below it, a table lists various AWS managed policies, with two specific ones selected: 'AWSDataPipeline_FullAccess' and 'AWSCodePipeline_FullAccess'. The browser status bar shows the URL https://us-east-1.console.aws.amazon.com/iamv2/home?region=us-east-1#/groups/create.

3. RDS Full Access

The screenshot shows the AWS IAM Management Console interface. On the left, the navigation pane is open with the 'User groups' section selected under 'Access management'. The main area displays two sections: 'Add users to the group - Optional (0)' and 'Attach permissions policies - Optional (Selected 1/771)'. In the 'Attach permissions policies' section, a single policy named 'AdministratorAccess-Amplify' is selected from a list of AWS managed policies. At the bottom right of the main area, there is a blue 'Create group' button.

4. DeviceFarm full Access

The screenshot shows the AWS IAM Management Console interface, similar to the previous one but with a different set of selected policies. The 'Attach permissions policies' section now shows multiple policies selected, including 'AWSDeviceFarmFullAccess', 'AWSIoTDeviceTesterForFreeRTOSFullAccess', 'AmazonSegeMakerEdgeDeviceFleetPolicy', 'AWSIoTDeviceDefenderEnableIoTLoggingMitigationAction', 'AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction', 'AWSIoTDeviceDefenderAddThingsToThingGroupMitigationAction', 'AWSIoTDeviceDefenderReplaceDefaultPolicyMitigationAction', 'AWSIoTDeviceDefenderUpdateDeviceCertMitigationAction', and 'AWSIoTDeviceDefenderUpdateCACertMitigationAction'. The rest of the interface is identical to the previous screenshot, with the 'Create group' button at the bottom right.

5. EC2 full Access

6. Role of Code Deploy

The screenshot shows the AWS IAM User Groups page. On the left, there's a sidebar with options like Identity and Access Management (IAM), Access management (User groups, Users, Roles, Policies, Identity providers, Account settings), Access reports (Access analyzer, Archive rules, Analyzers, Settings, Credential report, Organization activity, Service control policies (SCPs)), and Related consoles (IAM Identity Center). The main area has a search bar and a table titled "Attach permissions policies - Optional (Selected 2/771)". The table lists policies: "AmazonEC2FullAccess" (AWS managed, Provides full access), "AmazonEC2RoleforSSM" (AWS managed, This policy will soon be removed), "AmazonEC2RoleforAWSCodeDeploy" (AWS managed, Provides EC2 access), "AmazonEC2ContainerRegistryFullAccess" (AWS managed, Provides administrative access), "AmazonEC2ContainerRegistryReadOnly" (AWS managed, Provides read-only access), and "AmazonElasticMapReduceforEC2Role" (AWS managed, Default policy for the group). A note at the top says: "An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS. A user can belong to up to 10 groups." There are also "Create policy" and "Clear filters" buttons.

After then click on the Create Group.

This screenshot is identical to the one above, showing the AWS IAM User Groups page. The main difference is the presence of a large blue "Create Group" button at the bottom of the "Attach permissions policies" section. The rest of the interface, including the sidebar and the list of attached policies, remains the same.

After Creating a Group Click on the users and then you get the display like this

The screenshot shows the AWS IAM Management Console interface. On the left, there's a navigation sidebar with options like Identity and Access Management (IAM), Access management, Access reports, and Related consoles. The main content area is titled "Introducing the new Users list experience" with a message about redesigning the user list. It shows a table with columns for User name, Groups, Last activity, MFA, Password age, and Active key age. A search bar at the top says "Find users by username or access key". Below the table, it says "No resources to display". At the bottom right, there are buttons for "Delete" and "Add users". The status bar at the bottom shows the date and time as 17-09-2022 17:16.

Click on the Add User and you will get a form in that form in username field write the username and Select password or Access key.

The screenshot shows the "Add user" form in the AWS IAM Management Console. The title is "Add user". The first section is "Set user details" with a note that you can add multiple users at once. It has a "User name" field containing "Drashy" and a link to "Add another user". The next section is "Select AWS access type". It asks how users will primarily access AWS, mentioning programmatic access and the console. It includes a note about assumed roles and access keys. There are two options: "Access key - Programmatic access" (unchecked) and "Password - AWS Management Console access" (checked). The "Password" option is described as enabling a password for sign-in to the AWS Management Console. The "Console password" section shows "Autogenerated password" (radio button) selected, with a password "M1#i@2!3" in a text input field. A "Custom password" radio button is also present. Below this is a "Require password reset" checkbox, which is checked. A note says "User must create a new password at next sign-in" and "Users automatically get the IAMUserChangePassword policy to allow them to change their own password". At the bottom, there are "Required" and "Cancel" buttons, and a "Next: Permissions" button. The status bar at the bottom shows the date and time as 17-09-2022 17:15.

After that click on next: permissions button and click on add user to group.

You need permissions
You do not have the permission required to perform this operation. Ask your administrator to add permissions. Learn more
User: arn:aws:sts::281743333352:assumed-role/voclabs/user2100038-JASANI_MILANKUMAR_KANTIBHAI is not authorized to perform: iam>ListGroups on resource: arn:aws:iam::281743333352:group/ because no identity-based policy allows the iam>ListGroups action

Add user to group Copy permissions from existing user Attach existing policies directly

Click on the Tags button. And enter the key for security.

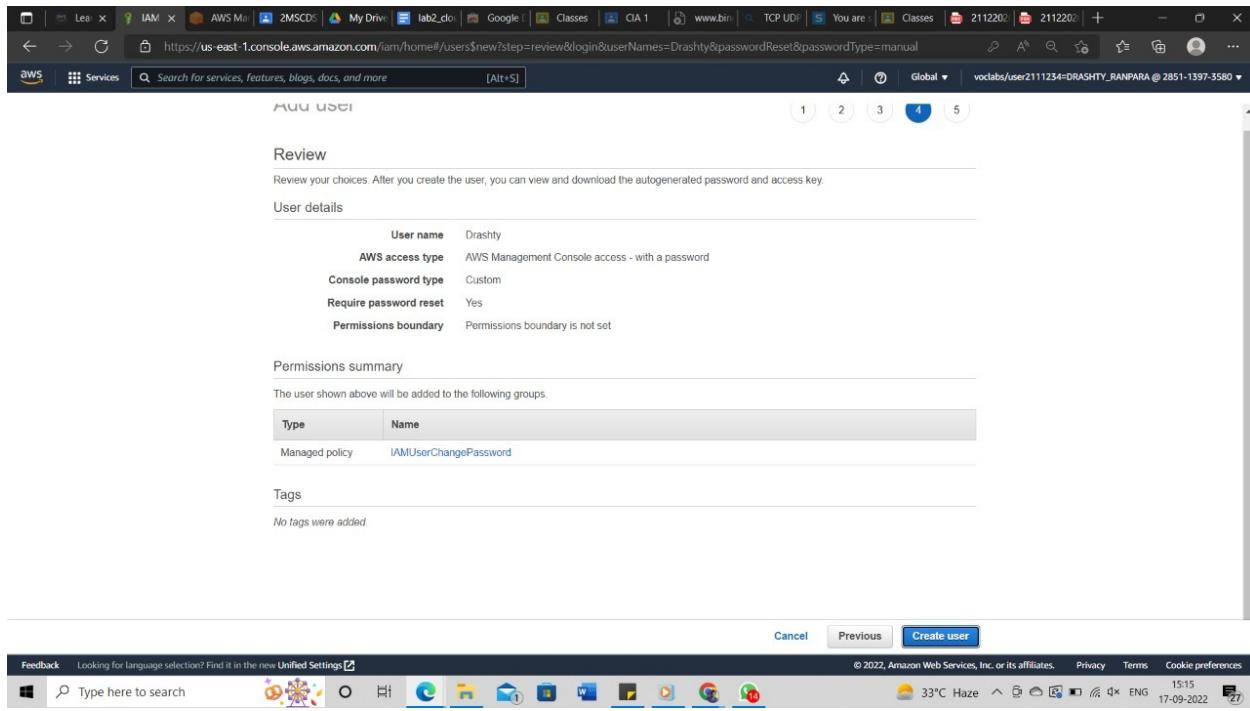
Add tags (optional)

IAM tags are key-value pairs you can add to your user. Tags can include user information, such as an email address, or can be descriptive, such as a job title. You can use the tags to organize, track, or control access for this user. Learn more

Key	Value (optional)	Remove
Add new key	Value	Remove

You can add 50 more tags.

Cancel Previous Next: Review



Then click on the Create user.

6. Draw a complete hierarchy of the user, user groups or policy in a form of a diagram

