

Exp 1a: Prerequisites

Xampp

1. Go to the official website of Xampp. <https://www.apachefriends.org/download.html>. Select the suitable version and complete the installation.

The screenshot shows the Apache Friends download page. At the top, there's a navigation bar with links for Apache Friends, Download, Hosting, Community, and About. A search bar and language selection (EN) are also present. The main content area has a large "Download" button. Below it, a section titled "XAMPP for Windows 8.0.30, 8.1.25 & 8.2.12" lists three versions with their checksums (md5, sha1), download links (Download (64 bit)), and sizes (144 Mb, 148 Mb, 149 Mb). To the right, a "Documentation/FAQs" sidebar provides links to Linux, Windows, and OS X FAQs. At the bottom, there are links for Requirements and More Downloads, and a note about unsupported platforms (Windows XP or 2003).

2. Once installation is complete, open the Xampp control panel. To host a php project locally we require to start the apache server.

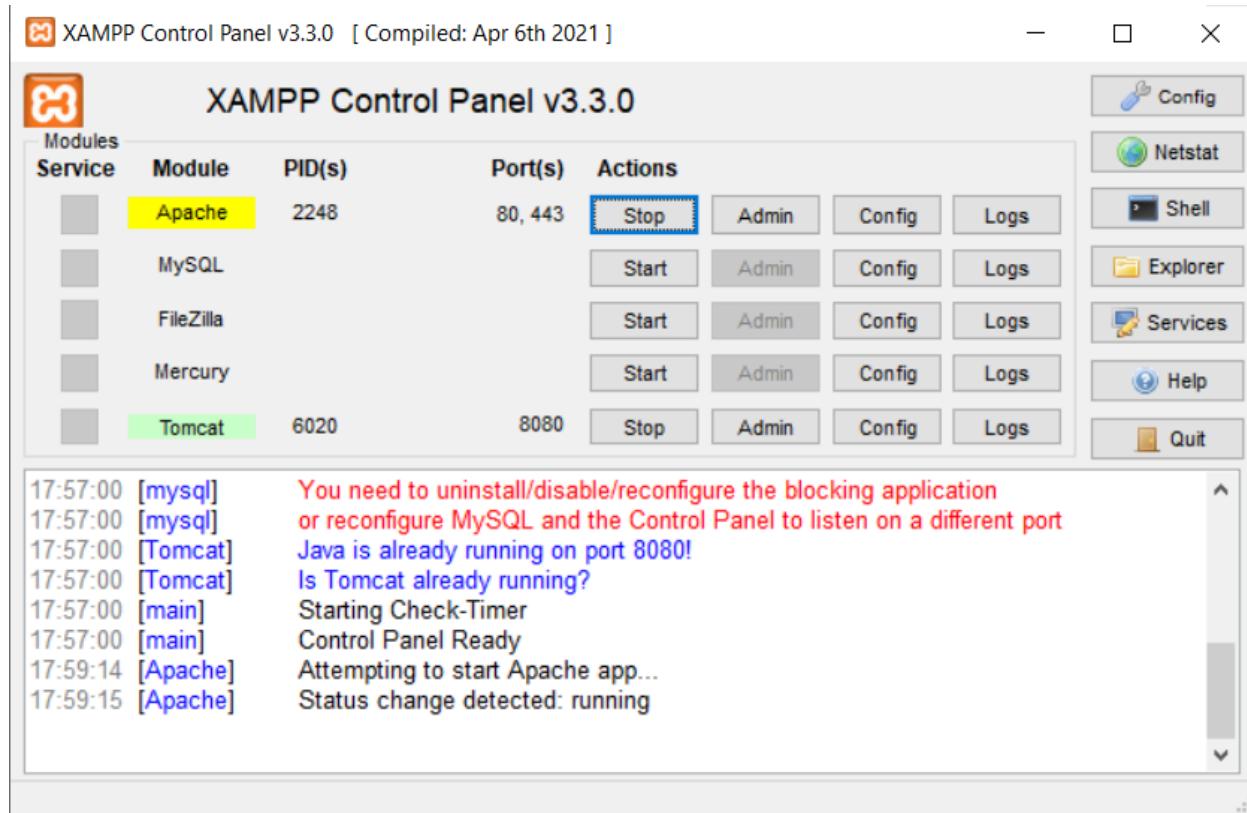
The screenshot shows the XAMPP Control Panel v3.3.0 interface. It features a table with columns for Service, Module, PID(s), Port(s), and Actions (Start, Admin, Config, Logs). Services listed include Apache, MySQL, FileZilla, Mercury, and Tomcat. Tomcat is highlighted in green. The log window at the bottom displays the following text in red:

```

17:57:00 [mysql] Port 3306 in use by "Unable to open process"!
17:57:00 [mysql] MySQL WILL NOT start without the configured ports free!
17:57:00 [mysql] You need to uninstall/disable/reconfigure the blocking application
17:57:00 [mysql] or reconfigure MySQL and the Control Panel to listen on a different port
17:57:00 [Tomcat] Java is already running on port 8080!
17:57:00 [Tomcat] Is Tomcat already running?
17:57:00 [main] Starting Check-Timer
17:57:00 [main] Control Panel Ready

```

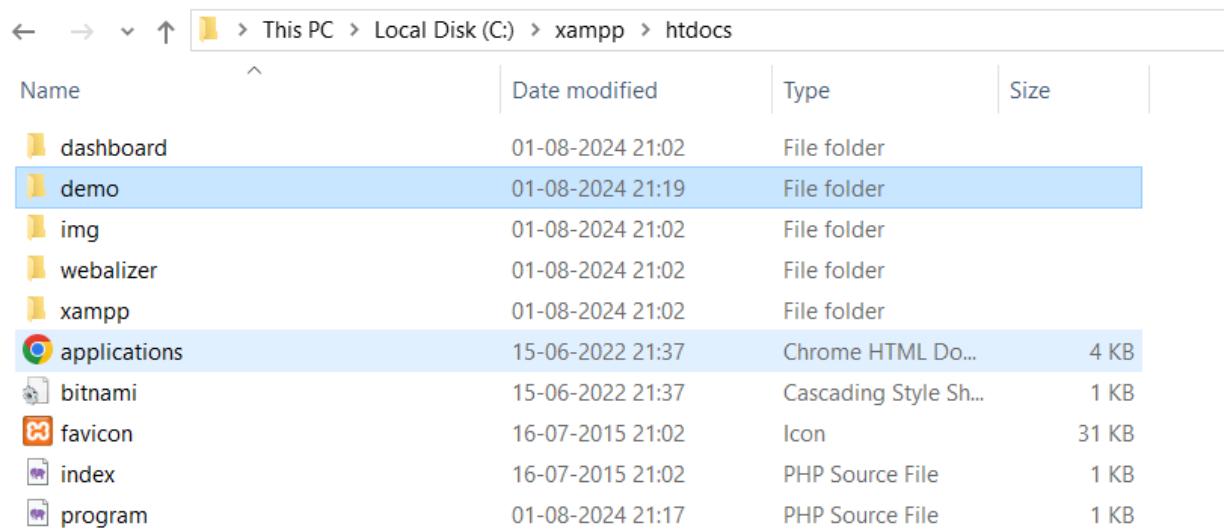
3. Click on start in front of apache and wait for the server to start.



4. We can now set up the php project. In the xampp folder in C drive there will be a folder named htdocs. Every project that we want to host locally should be present in htdocs.

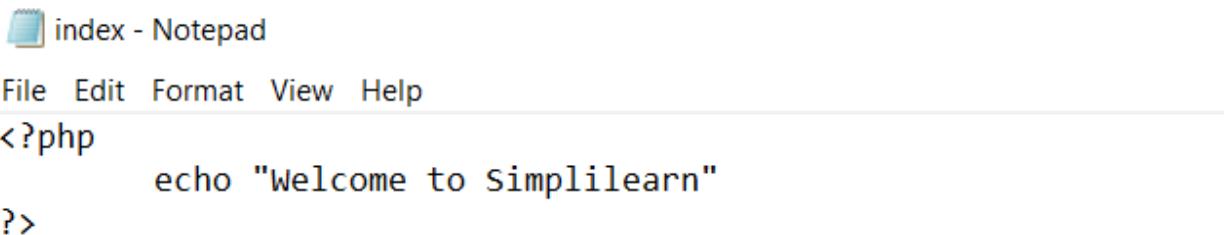
This PC > Local Disk (C:) > xampp >			
Name	Date modified	Type	Size
anonymous	01-08-2024 21:02	File folder	
apache	01-08-2024 21:02	File folder	
cgi-bin	01-08-2024 21:09	File folder	
contrib	01-08-2024 21:02	File folder	
FileZillaFTP	01-08-2024 21:09	File folder	
htdocs	01-08-2024 21:18	File folder	
img	01-08-2024 21:02	File folder	
install	01-08-2024 21:09	File folder	
licenses	01-08-2024 21:02	File folder	
locale	01-08-2024 21:02	File folder	
mailoutput	01-08-2024 21:02	File folder	
mailtodisk	01-08-2024 21:02	File folder	
MercuryMail	01-08-2024 21:09	File folder	
mysql	01-08-2024 21:03	File folder	
perl	01-08-2024 21:05	File folder	

5. We will create a project named demo inside htdocs. This demo folder will contain our php source code.



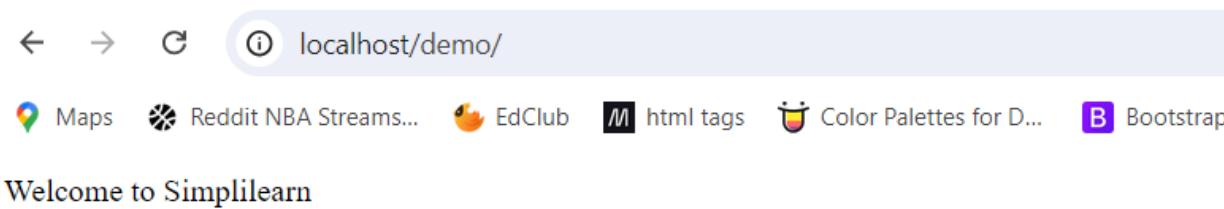
Name	Date modified	Type	Size
dashboard	01-08-2024 21:02	File folder	
demo	01-08-2024 21:19	File folder	
img	01-08-2024 21:02	File folder	
webalizer	01-08-2024 21:02	File folder	
xampp	01-08-2024 21:02	File folder	
applications	15-06-2022 21:37	Chrome HTML Do...	4 KB
bitnami	15-06-2022 21:37	Cascading Style Sh...	1 KB
favicon	16-07-2015 21:02	Icon	31 KB
index	16-07-2015 21:02	PHP Source File	1 KB
program	01-08-2024 21:17	PHP Source File	1 KB

6. Open the notepad and write a simple php script. Save this file inside the demo folder.



```
<?php
    echo "Welcome to Simplilearn"
?>
```

7. Go to your web browser and type “localhost/project_folder_name”, “localhost/demo” in this case. And we can see that our php script has been hosted locally using Xampp.



S3

1. Go to the AWS academy lab and search for s3 service.

The screenshot shows the AWS Academy lab interface. The search bar at the top contains 's3'. The main results section is titled 'Services' and shows three items: 'S3' (Scalable Storage in the Cloud), 'S3 Glacier' (Archive Storage in the Cloud), and 'AWS Snow Family' (Large Scale Data Transport). Below this, there's a 'Features' section with 'Imports from S3' and 'Feature spotlight'. A sidebar on the right is titled 'Create application' and includes fields for 'Applications', 'Region', and 'Originating account'. The bottom of the screen shows standard AWS navigation links like CloudShell, Feedback, and Copyright information.

2. In the s3 service select the create bucket option.

The screenshot shows the Amazon S3 service page. The main heading is 'Amazon S3' with the subtext 'Store and retrieve any amount of data from anywhere'. Below this is a brief description of what S3 is. On the right, there's a 'Create a bucket' button inside a box with explanatory text about buckets. At the bottom left, there's a 'How it works' section with a video thumbnail titled 'Introduction to Amazon S3'. The bottom of the screen shows standard AWS navigation links like CloudShell, Feedback, and Copyright information.

3. Select the name for bucket. Enter other details. Uncheck the block all public access option. Checking this box will give the 403 error when we try to access the website.

Block Public Access settings for this bucket

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to this bucket and its objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to this bucket or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

Block all public access
Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

- Block public access to buckets and objects granted through new access control lists (ACLs)**
S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.
- Block public access to buckets and objects granted through any access control lists (ACLs)**
S3 will ignore all ACLs that grant public access to buckets and objects.
- Block public access to buckets and objects granted through new public bucket or access point policies**
S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.
- Block public and cross-account access to buckets and objects through any public bucket or access point policies**
S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.

⚠️ Turning off block all public access might result in this bucket and the objects within becoming public
AWS recommends that you turn on block all public access, unless public access is required for specific and verified use cases such as static website hosting.

4. Use default setting for other options. Once configuration is completed, click on create bucket.

Successfully created bucket "www.d15c49.com"
To upload files and folders, or to configure additional bucket settings, choose [View details](#).

Server-side encryption is automatically applied to new objects stored in this bucket.

Encryption type: [Info](#)

- Server-side encryption with Amazon S3 managed keys (SSE-S3)
- Server-side encryption with AWS Key Management Service keys (SSE-KMS)
- Dual-layer server-side encryption with AWS Key Management Service keys (DSSE-KMS)
Secure your objects with two separate layers of encryption. For details on pricing, see [DSSE-KMS pricing](#) on the Storage tab of the [Amazon S3 pricing page](#).

Bucket Key
Using an S3 Bucket Key for SSE-KMS reduces encryption costs by lowering calls to AWS KMS. S3 Bucket Keys aren't supported for DSSE-KMS. [Learn more](#)

- Disable
- Enable

Advanced settings

💡 After creating the bucket, you can upload files and folders to the bucket, and configure additional bucket settings.

[Create bucket](#)

5. You can see the buckets created in General purpose buckets.

General purpose buckets (1) [Info](#) [All AWS Regions](#)

Buckets are containers for data stored in S3.

Name	AWS Region	IAM Access Analyzer	Creation date
www.d15c49.com	US East (N. Virginia) us-east-1	View analyzer for us-east-1	August 8, 2024, 18:53:28 (UTC+05:30)

6. Open the bucket, now we will upload files in our bucket. Select the upload button

The screenshot shows the AWS S3 console interface. At the top, there's a navigation bar with the AWS logo, 'Services' dropdown, 'Search' bar, and account information: 'N. Virginia' and 'vocabs/user3404112=SHARMA_RAKSHIT_KUMAR @ 3542-5662-2778'. Below the navigation is a breadcrumb trail: 'Amazon S3 > Buckets > www.d15c49.com'. The main content area is titled 'www.d15c49.com Info'. It has tabs for 'Objects' (which is selected), 'Properties', 'Permissions', 'Metrics', 'Management', and 'Access Points'. Under the 'Objects' tab, there's a toolbar with buttons for 'Copy S3 URI', 'Copy URL', 'Download', 'Open', 'Delete', 'Actions', 'Create folder', and a large orange 'Upload' button. A search bar says 'Find objects by prefix'. A table below shows 'No objects' found, with columns for 'Name', 'Type', 'Last modified', 'Size', and 'Storage class'. At the bottom of the table is another orange 'Upload' button. The footer includes links for 'CloudShell', 'Feedback', and copyright information: '© 2024, Amazon Web Services, Inc. or its affiliates.' and 'Cookie preferences'.

7. Select the files you want to upload in the bucket. Click on the upload button to upload files.

The screenshot shows the 'Upload' dialog within the AWS S3 console. At the top, it says 'Files and folders (2 Total, 504.0 B)' and 'All files and folders in this table will be uploaded.' There's a 'Remove' button and two buttons for 'Add files' and 'Add folder'. Below this is a search bar 'Find by name' and a table with one item: 'index.html' (Folder, text/html). The 'Destination' section shows 'Destination' set to 's3://www.d15c49.com'. Under 'Destination details', it says 'Bucket settings that impact new objects stored in the specified destination.' The 'Permissions' and 'Properties' sections are also visible. At the bottom of the dialog are 'Cancel' and 'Upload' buttons. The footer is identical to the previous screenshot, with 'CloudShell', 'Feedback', and copyright information.

8. You can see all the files uploaded in the bucket. Now go to the properties section to enable the static hosting option for the bucket.

The screenshot shows the AWS S3 console interface. At the top, there's a navigation bar with 'Services', a search bar, and account information ('N. Virginia' and 'voclabs/user3404112=SHARMA_RAKSHIT_KUMAR @ 3542-5662-2778'). Below the navigation bar, the path 'Amazon S3 > Buckets > www.d15c49.com' is shown. The main area displays the contents of the 'www.d15c49.com' bucket. A table lists two objects:

Name	Type	Last modified	Size	Storage class
error.html	html	August 8, 2024, 18:55:41 (UTC+05:30)	256.0 B	Standard
index.html	html	August 8, 2024, 18:55:42 (UTC+05:30)	248.0 B	Standard

9. Edit the static website hosting setting.

The screenshot shows the 'Properties' page for the 'www.d15c49.com' bucket in the AWS S3 console. The 'Static website hosting' section is expanded, showing the following configuration:

Setting	Value
Static website hosting	Disabled

Below this, there are sections for 'Transfer acceleration', 'Object Lock', and 'Requester pays', each with its own status and edit button.

10. Enable the static website hosting, select the index files and error files(optional). These will be the files you have uploaded in the bucket

The screenshot shows the AWS S3 console with the 'Static website hosting' tab selected. Under 'Hosting type', 'Host a static website' is chosen. The 'Index document' field contains 'index.html'. The 'Error document - optional' field contains 'error.html'. A note about public access is visible, stating: 'For your customers to access content at the website endpoint, you must make all your content publicly readable. To do so, you can edit the S3 Block Public Access settings for the bucket. For more information, see Using Amazon S3 Block Public Access.' The URL in the address bar is <https://docs.aws.amazon.com/console/s3/hostingstaticwebsite>.

11. Now we need to change the bucket policy in permissions. Ensure that block public access is off. Edit the bucket policy.

The screenshot shows the AWS S3 console. In the top navigation bar, 'Bucket policy' is selected. Under 'Block public access (bucket settings)', 'Block all public access' is set to 'Off'. Below this, the 'Bucket policy' section shows a note: 'The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts.' There is a 'No policy to display.' message. The URL in the address bar is <https://docs.aws.amazon.com/console/s3/hostingstaticwebsite>.

12. You can see examples of bucket policy. Use the appropriate bucket policy and enter your bucket name in it.

The screenshot shows the 'Edit bucket policy' page in the AWS Management Console. The policy is defined as follows:

```

1  2 < v {
3   "Version": "2012-10-17",
4   "Statement": [
5     {
6       "Sid": "PublicReadGetObject",
7       "Effect": "Allow",
8       "Principal": "*",
9       "Action": "s3:GetObject",
10      "Resource": "arn:aws:s3:::www.d15c49.com/*"
11    }
12  ]
13 }
14 ]
15 }

```

The right sidebar shows available actions like 'Edit statement', 'Add actions', and services like S3 and AMP.

13. Once the bucket policy is added, you can see the link for website in static website hosting.

The screenshot shows the 'Static website hosting' section of the bucket properties. It indicates that static website hosting is enabled and set to 'Bucket hosting'. The endpoint is listed as <http://www.d15c49.com.s3-website-us-east-1.amazonaws.com>.

14. On clicking the link you will be redirected to the hosted website.

The screenshot shows a browser window displaying the message 'Hello this is my website' at the top. Below the message, there is a navigation bar with links to various websites and tools.

Hello this is my website

Aim: To understand the benefits of Cloud Infrastructure and Setup AWS Cloud9 IDE, Launch AWS Cloud9 IDE and Perform Collaboration Demonstration.

1. Open the AWS account and search for Cloud9. Click on create environment.

The screenshot shows the AWS Cloud9 landing page. At the top right, there is a prominent orange "Create environment" button. Below it, there is descriptive text about AWS Cloud9 and its features. On the left, there is a section titled "How it works" with some explanatory text. On the right, there is a sidebar titled "Getting started" with several links: "Before you start" (2 min read), "Create an environment" (2 min read), "Working with environments" (15 min read), "Working with the IDE" (10 min read), and "Working with AWS Lambda" (5 min read). The bottom of the page includes standard AWS navigation links like CloudShell, Feedback, Privacy, Terms, and Cookie preferences.

2. Enter the name and other required configuration for creating an environment. In network settings, using the AWS system manager gives an error while creating the environment. It states there was an error creating IAM resources needed for SSM.

The screenshot shows the "Create environment" configuration page. Under "Network settings", there is a dropdown for "Timeout" set to "30 minutes". There are two options: "AWS Systems Manager (SSM)" (selected) and "Secure Shell (SSH)". Below this, there is a "VPC settings" section and a "Tags - optional" section. At the bottom, there is a callout box with an info icon stating: "The following IAM resources will be created in your account". It lists three items: "AWSServiceRoleForAWSCloud9" (a service-linked role for Cloud9 to call other AWS services), "AWSCloud9SSMAccessRole" (a service role for Cloud9 to access SSM), and "AWSCloud9SSMInstanceProfile" (an instance profile for Cloud9 instances to use SSM). The bottom of the page includes standard AWS navigation links like CloudShell, Feedback, Privacy, Terms, and Cookie preferences.

The screenshot shows the AWS Cloud9 VPC settings page. At the top, there's a note about optional tags. Below it, a box contains information about IAM resources that will be created: AWS Service Role for Cloud9, AWS Cloud9 SSM Access Role, and AWS Cloud9 SSM Instance Profile. A 'Create' button is at the bottom right. Below the main content, there are three error messages in red boxes:

- There was an error creating the IAM resources needed for SSM connection.
- You don't have the permission required to perform this operation. Ask your administrator to give you permissions.
- User: arn:aws:sts::354256622778:assumed-role/voclabs/user3404112=SHARMA_RAKSHIT_KUMAR is not authorized to perform: iam:CreateRole on resource: arn:aws:iam::354256622778:role/service-role/AWSCloud9SSMAccessRole because no identity-based policy allows the iam:CreateRole action

3. Use the Secure Shell option in Network settings.

The screenshot shows the AWS Cloud9 Network settings page. Under 'Connection', the 'Secure Shell (SSH)' option is selected, while 'AWS Systems Manager (SSM)' is unselected. A note at the bottom says 'Accesses environment directly via SSH, opens inbound ports'. Below the main content, there's a note about optional tags and a box containing information about IAM resources that will be created: AWS Service Role for Cloud9, AWS Cloud9 SSM Access Role, and AWS Cloud9 SSM Instance Profile. A 'Create' button is at the bottom right. Below the main content, there are two error messages in red boxes:

- There was an error creating the IAM resources needed for SSM connection.
- You don't have the permission required to perform this operation. Ask your administrator to give you permissions.

4. Once the configuration is complete, click on create environment to create a Cloud9 environment.

The screenshot shows the AWS Cloud9 environments management interface. On the left, there's a sidebar with links for 'My environments', 'Shared with me', and 'All account environments'. Below that is a 'Documentation' link. The main content area has a header 'Environments (1)' with a 'Create environment' button. A sub-header 'AWS Cloud9 > Environments' is present. A table lists one environment: 'MyEnvironment' (Status: Open, Type: EC2 instance, Connection: Secure Shell (SSH), Permission: Owner, ARN: arn:aws:sts::354256622778:assumed-role/voclabs/user3404112=SHARMA_RAKSHIT_KUMAR). At the bottom, there are navigation icons and a footer with copyright information and links for CloudShell, Feedback, Privacy, Terms, and Cookie preferences.

5. Click on the environment name to open the created Cloud9 Environment.

The screenshot shows the AWS Cloud9 IDE interface. The left sidebar shows a file tree with 'MyEnvironment' expanded, containing 'c9' and 'README.md'. The main area displays the 'Welcome' screen for 'MyEnvironment'. It features the 'AWS Cloud9' logo and the message 'Welcome to your development environment'. Below this is a 'Toolkit for AWS Cloud9' section with a description of its features. At the bottom is a terminal window with a bash prompt: 'bash - *p-172-31-5-244.e x Immediate voclabs:~/environment \$'. The interface includes standard menu options like File, Edit, Find, View, Go, Run, Tools, Window, Support, and a preview pane.

6. Open the aws account and search for IAM service.

The screenshot shows the AWS IAM Dashboard. On the left, a sidebar menu includes 'Identity and Access Management (IAM)', 'Dashboard', 'Access management' (with 'User groups', 'Users', 'Roles', 'Policies', 'Identity providers', 'Account settings'), 'Access reports' (with 'Access Analyzer', 'External access', 'Unused access', 'Analyzer settings', 'Credential report', 'Organization activity'), and 'CloudShell' and 'Feedback' buttons. The main content area has tabs for 'Security recommendations' (with a red notification dot) and 'IAM resources'. Under 'Security recommendations', there are two items: 'Add MFA for root user' (with a link to 'Add MFA') and 'Root user has no active access keys' (with a link to 'View all'). Under 'IAM resources', there are five categories: User groups (0), Users (0), Roles (2), Policies (0), and Identity providers (0). A 'What's new' section at the bottom right links to 'View all' changes. On the right side, there are sections for 'AWS Account' (Account ID: 975050293750, Account Alias: Create, Sign-in URL: https://975050293750.signin.aws.amazon.co/m/console) and 'Quick Links' (My security credentials, Manage your access keys, multi-factor authentication (MFA) and other credentials).

7. Go to the users tab. Click on create user to create a new user.

The screenshot shows the 'Users' page under the 'Identity and Access Management (IAM)' service. The sidebar is identical to the previous screenshot. The main content area shows a table titled 'Users (0) Info' with a note: 'An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.' Below the note is a search bar and a table header with columns: User name, Path, Group, Last activity, MFA, Password age, and Console last sign-in. A message 'No resources to display' is shown below the table. At the top right of the table area, there are 'Delete' and 'Create user' buttons. The footer contains standard AWS copyright and links.

8. Give the user name, select the “provide user access” checkbox. Also select the option “I want to create an IAM user”. Otherwise we will have to enable the Identity center and specify a user there.

User name
Rakshit

Provide user access to the AWS Management Console - optional

Are you providing console access to a person?

User type

- Specify a user in Identity Center - Recommended
- We recommend that you use Identity Center to provide console access to a person. With Identity Center, you can centrally manage user access to their AWS accounts and cloud applications.
- I want to create an IAM user
- We recommend that you create IAM users only if you need to enable programmatic access through access keys, service-specific credentials for AWS CodeCommit or Amazon Keyspaces, or a backup credential for emergency account access.

Console password

Autogenerated password

You can view the password after you create the user.

Custom password

Enter a custom password for the user.

- Must be at least 8 characters long
- Must include at least three of the following mix of character types: uppercase letters (A-Z), lowercase letters (a-z), numbers (0-9), and symbols ! @ # \$ % ^ & * () _ + - (hyphen) = [] { } []

Show password

Users must create a new password at next sign-in - Recommended

Users automatically get the IAMUserChangePassword policy to allow them to change their own password.

If you are creating programmatic access through access keys or service-specific credentials for AWS CodeCommit or Amazon Keyspaces, you can generate them after you create this IAM user. [Learn more](#)

Cancel Next

9. Next click on add user to group. If you do not have a existing group, select create group.

Step 1
Specify user details

Step 2
Set permissions

Step 3
Review and create

Step 4
Retrieve password

Set permissions

Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. [Learn more](#)

Permissions options

Add user to group

Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.

Copy permissions

Copy all group memberships, attached managed policies, and inline policies from an existing user.

Attach policies directly

Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.

Get started with groups

Create a group and select policies to attach to the group. We recommend using groups to manage user permissions by job function, AWS service access, or custom permissions. [Learn more](#)

Create group

Set permissions boundary - optional

Cancel Previous Next

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

10. Give the group name and policies if required, and create a group.

Create user group

Create a user group and select policies to attach to the group. We recommend using groups to manage user permissions by job function, AWS service access, or custom permissions. [Learn more](#)

User group name
Enter a meaningful name to identify this group.

Maximum 128 characters. Use alphanumeric and '+=,.@-_' characters.

Permissions policies (947)

Filter by Type
Search All ty... ▾

<input type="checkbox"/> Policy name	Type	Use...	Description
<input type="checkbox"/> AdministratorAccess	AWS managed ...	None	Provides full access to AWS services
<input type="checkbox"/> AdministratorAcce...	AWS managed	None	Grants account administrative perm
<input type="checkbox"/> AdministratorAcce...	AWS managed	None	Grants account administrative perm
<input type="checkbox"/> AlexaForBusinessD...	AWS managed	None	Provide device setup access to Alex
<input type="checkbox"/> AlexaForBusinessF...	AWS managed	None	Grants full access to AlexaForBusin
<input type="checkbox"/> AlexaForBusinessG...	AWS managed	None	Provide gateway execution access t

[Cancel](#) [Create user group](#)

11. Once the group is created, select the group in which the user should be added.

D15C user group created.

Step 2 Set permissions

Step 3 Review and create

Step 4 Retrieve password

Permissions options

Add user to group
Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.

Copy permissions
Copy all group memberships, attached managed policies, and inline policies from an existing user.

Attach policies directly
Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.

User groups (1/1)

<input checked="" type="checkbox"/> Group name	Users	Attached policies	Created
<input checked="" type="checkbox"/> D15C	0	-	2024-08-08 (Now)

[Set permissions boundary - optional](#)

[Cancel](#) [Previous](#) [Next](#)

12. Recheck all the configuration and details of the user and click on create user.

The screenshot shows the 'User details' section with the user name 'Rakshit'. It also displays the 'Permissions summary' table, which includes two entries: 'D15C' (Group, Permissions group) and 'IAMUserChangePassword' (AWS managed, Permissions policy). The 'Tags - optional' section indicates no tags are associated with the resource. A 'Create user' button is visible at the bottom right.

User details

User name	Rakshit	Console password type	Custom password
			Require password reset Yes

Permissions summary

Name	Type	Used as
D15C	Group	Permissions group
IAMUserChangePassword	AWS managed	Permissions policy

Tags - optional
Tags are key-value pairs you can add to AWS resources to help identify, organize, or search for resources. Choose any tags you want to associate with this user.
No tags associated with the resource.
[Add new tag](#)
You can add up to 50 more tags.

[Cancel](#) [Previous](#) [Create user](#)

The screenshot shows the 'Console sign-in details' section, which includes the 'Console sign-in URL' (https://975050293750.signin.aws.amazon.com/console), 'User name' ('Rakshit'), and 'Console password' (represented by a masked string). An 'Email sign-in instructions' link is also present. Navigation links for 'IAM > Users > Create user' are at the top left, and 'View user' and 'Return to users list' buttons are at the bottom right.

Retrieval password
You can view and download the user's password below or email users instructions for signing in to the AWS Management Console. This is the only time you can view and download this password.

Console sign-in details

Console sign-in URL
<https://975050293750.signin.aws.amazon.com/console>

User name
[Rakshit](#)

Console password
[*****](#) [Show](#)

[Email sign-in instructions](#)

[Cancel](#) [Download .csv file](#) [Return to users list](#)

13. After creation of the user, go to the user groups tab and select the group in which the user has been added. Navigate to the permissions tab. Click on add permissions and attach policy.

The screenshot shows the AWS IAM User Groups page. On the left, the navigation menu includes 'Identity and Access Management (IAM)', 'Access management' (selected), 'User groups', 'Users', 'Roles', 'Policies', 'Identity providers', and 'Account settings'. Under 'Access reports', it lists 'Access Analyzer', 'External access', 'Unused access', 'Analyzer settings', 'Credential report', and 'Organization activity'. At the bottom, there are links for 'CloudShell' and 'Feedback'.

The main content area displays the 'D15C' user group. The 'Summary' section shows the group name 'D15C', creation time 'August 08, 2024, 22:18 (UTC+05:30)', and ARN 'arn:awsiam:975050293750:group/D15C'. Below this, tabs for 'Users (1)', 'Permissions', and 'Access Advisor' are present. The 'Users in this group (1)' section shows a single user 'Rakshit'. At the bottom right of the main content area, there are links for '© 2024, Amazon Web Services, Inc. or its affiliates.', 'Privacy', 'Terms', and 'Cookie preferences'.

14. Search for the “AWSCloud9EnvironmentMember” policy and attach it.

The screenshot shows the 'Attach permission policies to D15C' page. The top navigation bar shows 'IAM > User groups > D15C > Add permissions'. The main content area has a heading 'Attach permission policies to D15C' and a sub-section 'Current permissions policies (0)'. Below this is a search bar with 'cloud9' and a filter 'All types'. A table lists four policies: 'AWSCloud9Administrator' (selected), 'AWSCloud9EnvironmentMember' (selected), 'AWSCloud9SSMInstanceProfile', and 'AWSCloud9User'. The 'AWSCloud9EnvironmentMember' row is highlighted with a blue background. At the bottom right, there are 'Cancel' and 'Attach policies' buttons.