



School of Computer Science, Engineering and Applications(SCSEA)  
B.C.A. TY (CCSA)  
Subject : Infrastructure Orchestration (P)

Name of the Student: Prakhar Anil Sharma

PRN: 20220801121

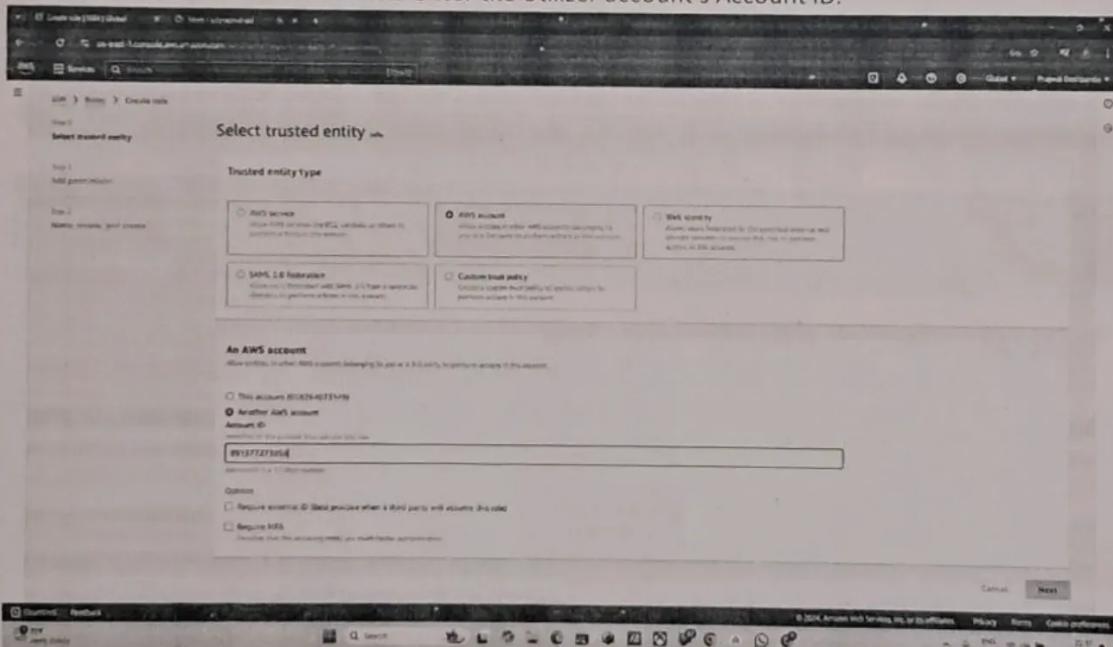
Title of Practical : Cross Account Access

Step 1: Create a Role in the Provider Account

1. Log in to the AWS Console with the Provider account (the account you want to give access to). In my case (Prajwal Deshpande)
2. Navigate to the IAM Service.
3. In the left navigation pane, click on Roles.
4. Click on Create Role.

Step 2: Set Up Trusted Entity

- In the Trusted Entity Type section, select AWS Account. IAMRoleTrustedEntityType
- Scroll down to the An AWS Account section.
- Choose Another AWS Account and enter the Utilizer account's Account ID.



Step 3: Add Permissions

- In the Add Permissions section, filter the permissions by AWS Managed - Job Function
- In the search bar, search for ReadOnlyAccess.

PRN: 20220801121



**School of Computer Science, Engineering and Applications(SCSEA)**  
**B.C.A. TY (CCSA)**  
**Subject : Infrastructure Orchestration (P)**

**Name of the Student:** Prakhar Anil Sharma

**PRN:** 20220801121

**Title of Practical :** Cross Account Access

- Select the ReadOnlyAccess policy to provide read-only access to the Utilizer account.

The screenshot shows the AWS IAM 'Create role' wizard at Step 3: Add permissions. The 'Add permissions' section is open, showing a search bar with 'ReadOnlyAccess' and a results table. One result, 'ReadOnlyAccess', is selected and highlighted in blue. The table includes columns for Policy name, Type, and Description. The description for 'ReadOnlyAccess' states: 'Provides read-only access to AWS service...'. At the bottom right of the dialog, there are 'Cancel', 'Previous', and 'Next' buttons, with 'Next' being the last one in the sequence.

**Step 4: Name, Review, and Create Role**

- Enter a name and description for the role.
- Review the role configuration and click on Create Role.



**School of Computer Science, Engineering and Applications(SCSEA)**  
**B.C.A. TY (CCSA)**  
**Subject : Infrastructure Orchestration (P)**

**Name of the Student:** Prakhar Anil Sharma

**PRN:** 20220801121

**Title of Practical :** Cross Account Access

Role details

Role name: BCA-CCSA-TY-1121

Description: Cross Account Task

```
1: {
2:     "Version": "2012-10-17",
3:     "Statement": [
4:         {
5:             "Effect": "Allow",
6:             "Action": "sts:AssumeRole",
7:             "Principal": {
8:                 "AWS": "891377273858"
9:             },
10:            "Condition": {}
11:        }
12:    ]
13: }
```

Step 2: Add permissions

Role BCA-CCSA-TY-1121 created.

Identity and Access Management (IAM)

Roles (8) Info

Role name	Trusted entities	Last activity
AWSServiceRoleForOrganizations	AWS Service: organizations (Service-Linked Role)	1 hour ago
AWSServiceRoleForRDS	AWS Service: rds (Service-Linked Role)	1 hour ago
AWSServiceRoleForSupport	AWS Service: support (Service-Linked Role)	-
AWSServiceRoleForTrustedAdvisor	AWS Service: trustedadvisor (Service-Linked Role)	-
BCA-CCSA-TY-1121	Account: 891377273858	-
cloudformation	AWS Service: cloudformation	26 days ago
rds-monitoring-role	AWS Service: monitoring.rds	-
RoleForCloudTrail	AWS Service: cloudtrail	37 days ago

Temporary credentials



**School of Computer Science, Engineering and Applications(SCSEA)**  
**B.C.A. TY (CCSA)**  
**Subject : Infrastructure Orchestration (P)**

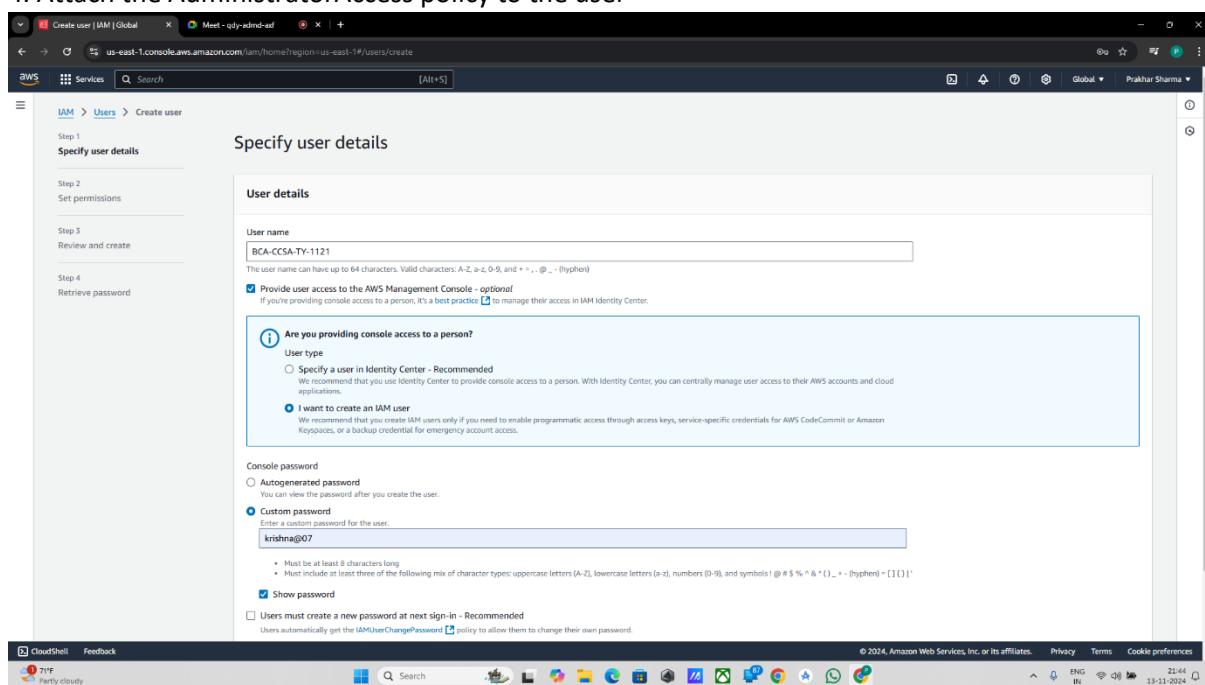
**Name of the Student:** Prakhar Anil Sharma

**PRN:** 20220801121

**Title of Practical :** Cross Account Access

**Step 5: Create an IAM User in the Utilizer Account**

1. Log in to the Utilizer account.( In this case Prakhar Sharma)
2. Go to the IAM Service and create a new IAM User.
3. Name the user, check the Provide user access to the AWS Management Console field, and then provide a password.
4. Attach the AdministratorAccess policy to the user



The screenshot shows the 'Create user' wizard in the AWS IAM service. The user is on Step 1: Specify user details. The 'User name' field contains 'BCA-CCSA-TY-1121'. The 'Provide user access to the AWS Management Console' checkbox is checked. The 'I want to create an IAM user' checkbox is also checked. Under 'Console password', 'Custom password' is selected with the value 'krishna@07'. The 'Show password' checkbox is checked. The 'Users must create a new password at next sign-in - Recommended' checkbox is checked. The browser status bar at the bottom indicates it's from 'aws.amazon.com' and shows the date '11-11-2024'.



# School of Computer Science, Engineering and Applications(SCSEA)

## B.C.A. TY (CCSA)

### Subject : Infrastructure Orchestration (P)

Name of the Student: Prakhar Anil Sharma

PRN: 20220801121

Title of Practical : Cross Account Access

Step 1: Specify user details

Step 2: Set permissions

Step 3: Review and create

Step 4: Retrieve password

Permissions options

- Add user to group
- Copy permissions
- Attach policies directly

Permissions policies (1/1257)

Policy name	Type	Attached entities
AccessAnalyzerServiceRolePolicy	AWS managed	0
<u>AdministratorAccess</u>	AWS managed - job function	0
AdministratorAccess-Amplify	AWS managed	0
AdministratorAccess-AWSElasticBeanstalk	AWS managed	0
AlexaForBusinessDeviceSetup	AWS managed	0
AlexaForBusinessFullAccess	AWS managed	0
AlexaForBusinessGatewayExecution	AWS managed	0
AlexaForBusinessIfrsizeDelegatedAccessPolicy	AWS managed	0

Step 1: Specify user details

Step 2: Set permissions

Step 3: Review and create

Step 4: Retrieve password

User details

User name BCA-CCSA-TY-1121	Console password type Custom password	Require password reset No
-------------------------------	--	------------------------------

Permissions summary

Name <u>AdministratorAccess</u>	Type AWS managed - job function	Used as Permissions policy
------------------------------------	------------------------------------	-------------------------------

Tags - optional

Add new tag

Cancel Previous Create user

PRN: 20220801121

5



D Y PATIL  
INTERNATIONAL  
UNIVERSITY  
AKURDI PUNE

**School of Computer Science, Engineering and Applications(SCSEA)**  
**B.C.A. TY (CCSA)**  
**Subject : Infrastructure Orchestration (P)**

**Name of the Student:** Prakhar Anil Sharma

**PRN:** 20220801121

**Title of Practical :** Cross Account Access

User created successfully

You can view and download the user's password and email instructions for signing in to the AWS Management Console.

IAM > Users > Create user

Step 1 Specify user details

Step 2 Set permissions

Step 3 Review and create

Step 4 Retrieve password

Retrieve password

Console sign-in details

Console sign-in URL: https://prakhar7sharma.signin.aws.amazon.com/console

User name: BCA-CCSA-TY-1121

Console password: \*\*\*\*\* Show

Cancel Download .csv file Return to users list

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences 21:46 ENG IN 11-11-2024

**Step 6: Switch Role in the Utilizer Account**

You are currently using the improved sign in UI experience. The improved sign in experience will launch soon. During this time, you can still change back to legacy sign in using the dropdown in the upper right corner.

IAM user sign in

Account ID (12 digits) or account alias: 891377273858

IAM username: BCA-CCSA-TY-1121

Password: krishna@07

Show Password Having trouble?

Sign in

Sign in using root user email

Create a new AWS account

Remember this account

By continuing, you agree to AWS Customer Agreement or other agreement for AWS services, and the Privacy Notice. This site uses essential cookies. See our [Cookie Notice](#) for more information.

Amazon Lightsail

Lightsail is the easiest way to get started on AWS

Learn more »

aws

CloudShell Feedback © 2024 Amazon Web Services, Inc. or its affiliates. All rights reserved. 21:49 ENG IN 11-11-2024

PRN: 20220801121



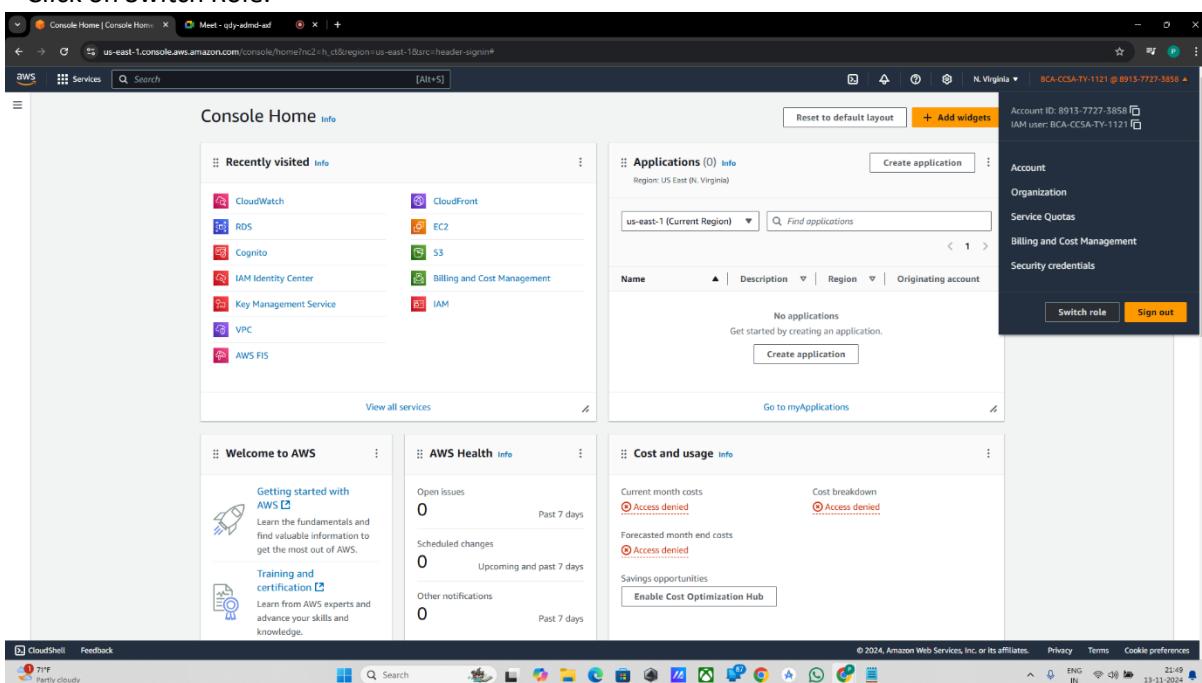
**School of Computer Science, Engineering and Applications(SCSEA)**  
**B.C.A. TY (CCSA)**  
**Subject : Infrastructure Orchestration (P)**

**Name of the Student:** Prakhar Anil Sharma

**PRN:** 20220801121

**Title of Practical :** Cross Account Access

- Log in with the IAM user you just created in the Utilizer account.
- In the top-right corner, click on the Account Name.
- Click on Switch Role.



The screenshot shows the AWS Console Home page. At the top right, there is a dark sidebar with the account ID and name (BCA-CCSA-TY-1121) and a 'Switch role' button. The main content area displays various AWS services like CloudWatch, CloudFront, RDS, EC2, Cognito, S3, IAM, Key Management Service, VPC, and AWS FIS. Below these are sections for 'Welcome to AWS' (Getting started with AWS, Training and certification), 'AWS Health' (Open issues, Scheduled changes, Other notifications), and 'Cost and usage' (Current month costs, Forecasted month end costs, Savings opportunities). The bottom of the screen shows the Windows taskbar with several pinned icons.

1. Enter the Provider Account ID and the Role Name (the one created in the Provider account).



## School of Computer Science, Engineering and Applications(SCSEA) B.C.A. TY (CCSA) Subject : Infrastructure Orchestration (P)

Name of the Student: Prakhar Anil Sharma

PRN: 20220801121

Title of Practical : Cross Account Access

2. Enter a Display Name and choose a Display Color if desired.

Switch Role  
Switching roles enables you to manage resources across Amazon Web Services accounts using a single user. When you switch roles, you temporarily take on the permissions assigned to the new role. When you exit the role, you give up those permissions and get your original permissions back. [Learn more](#)

Account ID  
The 12-digit account number or the alias of the account in which the role exists.  
058264073149

IAM role name  
The name of the role that you want to assume which can be found at the end of the role's ARN. For example, provide the TestRole role name from the following role ARN: arn:aws:iam::123456789012:role/TestRole  
BCA-CCSA-TY-1121

Display name - optional  
This name will appear in the console navigation bar when active. Choose a name to help identify the permission set assigned to the role.  
BCA-CCSA-TY-1121 @ 058264073149

Display color - optional  
The selected color displays in the console navigation when this role is active  
Red

Cancel Switch Role

Console Home

Recently visited

- IAM
- Billing and Cost Management
- S3
- EC2
- CloudFront
- AWS FIS
- VPC
- Key Management Service
- IAM Identity Center
- Cognito
- RDS
- CloudWatch

Welcome to AWS

Getting started with AWS

Training and certification

Cost and usage

Open issues 0 Past 7 days

Scheduled changes 0 Upcoming and past 7 days

Other notifications 0 Past 7 days

AWS Health

Cost breakdown

Access denied

Forecasted month end costs

Access denied

Savings opportunities

Enable Cost Optimization Hub

PRN: 20220801121



**School of Computer Science, Engineering and Applications(SCSEA)**  
**B.C.A. TY (CCSA)**  
**Subject : Infrastructure Orchestration (P)**

**Name of the Student:** Prakhar Anil Sharma

**PRN:** 20220801121

**Title of Practical :** Cross Account Access

**Step 7: Verify Access**

1. To verify access, create an S3 bucket in the Provider account.

- o Enter a unique name for the bucket.

The screenshot shows the 'Create bucket' wizard on the AWS S3 console. The 'General configuration' step is active. In the 'Bucket type' section, 'General purpose' is selected. The 'Bucket name' field contains 's3-prakhar-bucket'. Below the name field, there's a note about uniqueness and naming rules. Under 'Object Ownership', 'ACLs disabled (recommended)' is selected. The bottom of the screen shows the Windows taskbar with various icons and system status.



**School of Computer Science, Engineering and Applications(SCSEA)**  
**B.C.A. TY (CCSA)**  
**Subject : Infrastructure Orchestration (P)**

**Name of the Student:** Prakhar Anil Sharma      **PRN:** 20220801121

**Title of Practical :** Cross Account Access

A screenshot of a web browser displaying the AWS S3 service. The URL is "us-east-1.console.aws.amazon.com/s3/buckets?region=us-east-1&amp;bucketType=general". The page shows a success message: "Successfully created bucket 's3-prajwal-bucket'". Below this, there's an "Account snapshot - updated every 24 hours" section and a table of "General purpose buckets". The table has one row: "s3-prajwal-bucket" (Name), "US East (N. Virginia) us-east-1" (AWS Region), and "November 13, 2024, 22:00:39 (UTC+05:30)" (Creation date). The browser's address bar shows "S3 buckets | S3 | us-east-1" and the title "Meet - qdy-admnd-ad". The status bar at the bottom right shows "22:00", "ENG IN", and "13-11-2024".

Now, to verify if cross-account access works, return to the Utilizer account IAM user and navigate to the S3 service to check the bucket you just created.



D Y PATIL  
INTERNATIONAL  
UNIVERSITY  
AKURDI PUNE

**School of Computer Science, Engineering and Applications(SCSEA)**  
**B.C.A. TY (CCSA)**  
**Subject : Infrastructure Orchestration (P)**

**Name of the Student:** Prakhar Anil Sharma

**PRN:** 20220801121

**Title of Practical :** Cross Account Access

The screenshot shows the AWS S3 console with the 'General purpose buckets' tab selected. A new bucket named 'c3-provider-bucket' has been created. The details shown include the bucket name, the AWS Region (US East (N. Virginia)), and the creation date (November 1, 2024). There is also a link to 'IAM Access Analyzer'.

This screenshot shows the same AWS S3 console interface, but the bucket 'c3-provider-bucket' is now listed among the existing buckets. It includes columns for Name, AWS Region, and Creation Date.

You can see We are able to see the bucket which we created at Providers Account.

*[Handwritten signature]*  
28/11/23

PRN: 20220801121