

## Practical no: 3

Name: Saloni Vishwakarma

Batch-Roll no: C1-13

Subject: Introduction to Cloud Security Lab

Date of Execution: 09/02/2024

**Aim:** Configure AWS Identity and Access Management (IAM) Service.

### TASK 1:

The screenshot shows the 'Specify user details' step of the AWS IAM 'Create user' wizard. The URL is [us-east-1.console.aws.amazon.com/iam/home?region=eu-north-1#/users/create](https://us-east-1.console.aws.amazon.com/iam/home?region=eu-north-1#/users/create). The left sidebar shows steps: Step 1 (Specify user details), Step 2 (Set permissions), Step 3 (Review and create), and Step 4 (Retrieve password). The main form has a 'User name' field containing 'EmergencyAccess'. A note below it says: 'The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = , . @ \_ - (hyphen)'. A checked checkbox says: 'Provide user access to the AWS Management Console - optional'. A tooltip for console access asks: 'Are you providing console access to a person?' with options: 'Specify a user in Identity Center - Recommended' (radio button unselected) and 'I want to create an IAM user' (radio button selected). The bottom of the screen shows the Windows taskbar with various icons and the date/time: 09-02-2024, 14:27, ENG IN.

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**

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.  
**EmergencyAccessGroup**

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

**Permissions policies (1/912)**

Policy name	Type	Use...	Description
<input checked="" type="checkbox"/> AdministratorAccess	AWS managed	None	Provides full access to AWS services
<input type="checkbox"/> AdministratorAcc...	AWS managed	None	Grants account administrative perm
<input type="checkbox"/> AdministratorAcc...	AWS managed	None	Grants account administrative perm

**Create user group**

us-east-1.console.aws.amazon.com/iam/home?region=eu-north-1#/users/create

EmergencyAccessGroup user group created.

Specify user details

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](#)

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)

Group name	Users	Attached policies	Created
EmergencyAccessGroup	0	AdministratorAccess	2024-02-09 (Now)

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences NIFTY +0.18% ENG IN 14:33 09-02-2024

us-east-1.console.aws.amazon.com/iam/home?region=eu-north-1#/users/create

EmergencyAccessGroup user group created.

IAM > Users > Create user

Step 1 Specify user details

Step 2 Set permissions

Step 3 Review and create

Step 4 Retrieve password

**Review and create**

Review your choices. After you create the user, you can view and download the autogenerated password, if enabled.

**User details**

User name	EmergencyAccess	Console password type	Autogenerated	Require password reset	No
-----------	-----------------	-----------------------	---------------	------------------------	----

**Permissions summary**

Name	Type	Used as
EmergencyAccessGroup	Group	Permissions group

Tags - optional

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences 25°C Haze ENG IN 14:35 09-02-2024

us-east-1.console.aws.amazon.com/iam/home?region=eu-north-1#/users/create

User created successfully

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

Step 1 Specify user details

Step 2 Set permissions

Step 3 Review and create

Step 4 Retrieve password

**Retrieve 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**

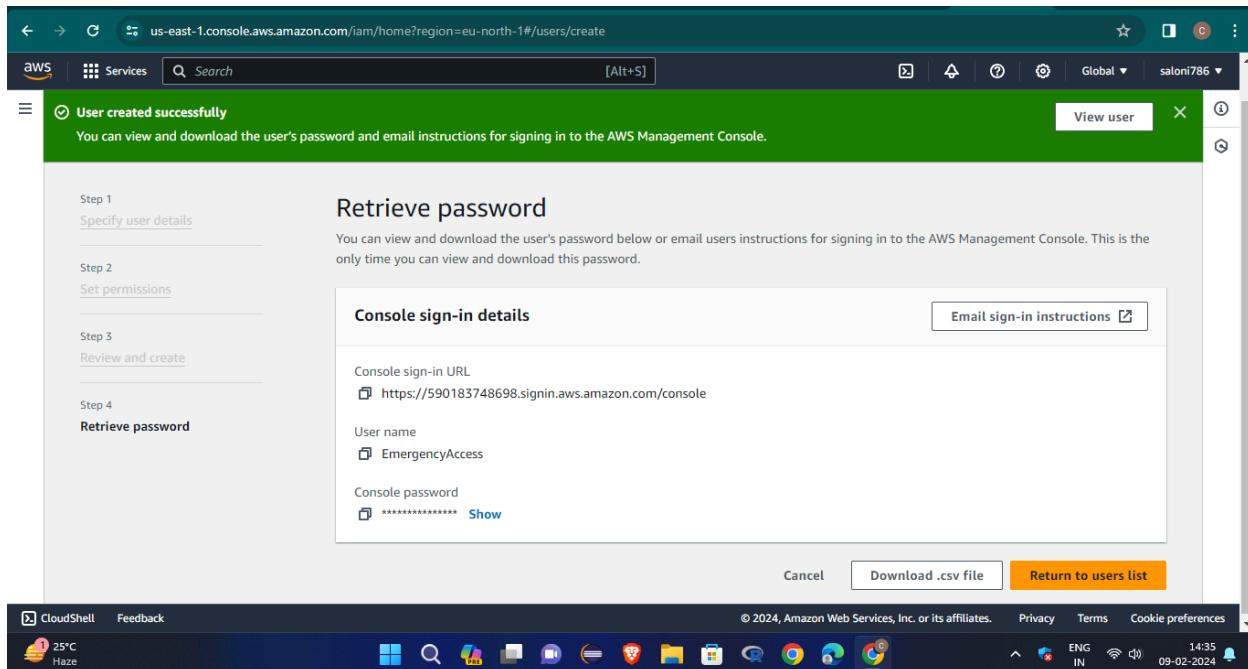
Console sign-in URL: https://590183748698.signin.aws.amazon.com/console

User name: EmergencyAccess

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 25°C Haze ENG IN 14:35 09-02-2024 saloni786



us-east-1.console.aws.amazon.com/iam/home?region=eu-north-1#/users/details/EmergencyAccess?section=permissions

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

User groups

**Users**

Roles

Policies

Identity providers

Account settings

Access reports

Access Analyzer

External access

Unused access

IAM > Users > EmergencyAccess

**EmergencyAccess** Info

Delete

**Summary**

ARN: arn:aws:iam::590183748698:user/EmergencyAccess	Console access: Enabled without MFA	Access key 1: Create access key
Created: February 09, 2024, 14:35 (UTC+05:30)	Last console sign-in: Never	

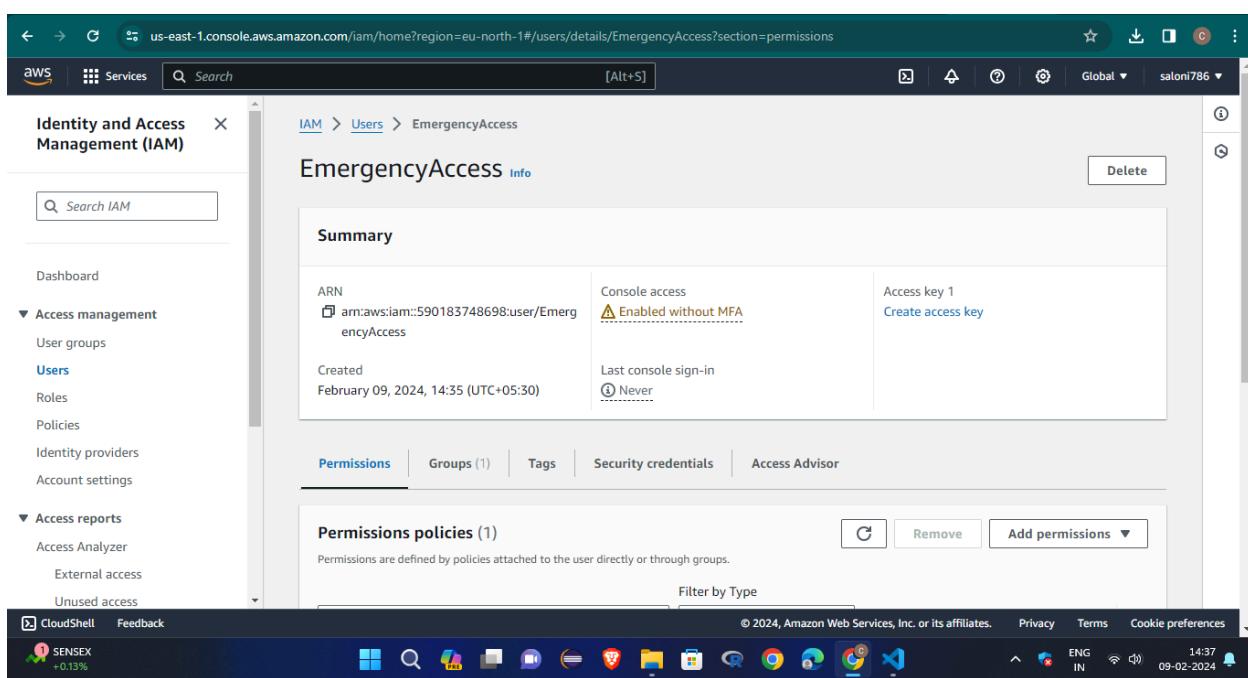
Permissions Groups (1) Tags Security credentials Access Advisor

**Permissions policies (1)**

Permissions are defined by policies attached to the user directly or through groups.

Add permissions

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences SENSEX +0.13% ENG IN 14:37 09-02-2024 saloni786



[us-east-1.console.aws.amazon.com/iam/home?region=eu-north-1#/users/details/EmergencyAccess?section=permissions](https://us-east-1.console.aws.amazon.com/iam/home?region=eu-north-1#/users/details/EmergencyAccess?section=permissions)

AWS Services Search [Alt+S] Global saloni786

### Identity and Access Management (IAM)

Permissions Groups (1) Tags Security credentials Access Advisor

#### Permissions policies (1)

Permissions are defined by policies attached to the user directly or through groups.

Filter by Type  All types

Policy name	Type	Attached via
AdministratorAccess	AWS managed - job function	Group EmergencyAccessGroup

#### Permissions boundary (not set)

#### Generate policy based on CloudTrail events

You can generate a new policy based on the access activity for this user, then customize, create, and attach it to this role. AWS uses your CloudTrail events to identify the services and actions used and generate a policy. [Learn more](#)

Generate policy

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences ENG IN 14:38 09-02-2024

SENSEX +0.13%

CloudShell Feedback

[us-east-1.console.aws.amazon.com/iam/home?region=eu-north-1#/roles](https://us-east-1.console.aws.amazon.com/iam/home?region=eu-north-1#/roles)

AWS Services Search [Alt+S] Global saloni786

### Identity and Access Management (IAM)

IAM > Roles

#### Roles (2) Info

An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.

Role name	Trusted entities	Last activity
AWSServiceRoleForSupport	AWS Service: support (Service-Linker)	-
AWSServiceRoleForTrustedAdvisor	AWS Service: trustedadvisor (Service-Linker)	-

#### Roles Anywhere Info

Authenticate your non AWS workloads and securely provide access to AWS services.

Manage

Nifty bank +0.00%

CloudShell Feedback

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences ENG IN 14:39 09-02-2024

us-east-1.console.aws.amazon.com/iam/home?region=eu-north-1#/roles/create

IAM > Roles > Create role

Step 1  
Select trusted entity

Step 2  
Add permissions

Step 3  
Name, review, and create

### Select trusted entity Info

#### Trusted entity type

AWS service  
Allow AWS services like EC2, Lambda, or others to perform actions in this account.

AWS account  
Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.

Web identity  
Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.

SAML 2.0 federation  
Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.

Custom trust policy  
Create a custom trust policy to enable others to perform actions in this account.

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences 25°C Haze ENG IN 14:42 09-02-2024

us-east-1.console.aws.amazon.com/iam/home?region=eu-north-1#/roles/create

IAM > Roles > Create role

Step 1  
Select trusted entity

Step 2  
Add permissions

Step 3  
Name, review, and create

### Add principal

Specify the principal type and ARN to add for the selected service.

Principal type: IAM Roles

ARN: arn:aws:iam::590183748698:user/EmergencyAccess

Cancel Add principal

AssumeRoleWithSAML info  
AssumeRoleWithWebIdentity info  
DecodeAuthorizationMessage info  
Context info  
SourceIdentity info  
Level - tagging  
Session info  
principal  
condition (optional)

Preview external access

Cancel Next

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences 25°C Haze ENG IN 14:44 09-02-2024

Custom trust policy

Create a custom trust policy to enable others to perform actions in this account.

```
1 ▼ {
  2   "Version": "2012-10-17",
  3   "Statement": [
  4     {
  5       "Sid": "Statement1",
  6       "Effect": "Allow",
  7       "Principal": [
  8         "arn:aws:iam::590183748690:user/EmergencyAccess"
  9       ],
  10      "Action": "sts:AssumeRole"
  11    }
  12  ]
  13 }
```

Edit statement Statement1 Remove

Add actions for STS

Filter actions

GetSessionToken Info

Access level - read or write

AssumeRole Info

AssumeRoleWithSAML Info

AssumeRoleWithWebIdentity Info

DecodeAuthorizationMessage Info

SetContext Info

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences ENG IN 14:45 09-02-2024

us-east-1.console.aws.amazon.com/iam/home?region=eu-north-1#/roles/create?trustedEntityType=CUSTOM\_TRUST\_POLICY

<input type="checkbox"/>	Name	Type	Description
<input type="checkbox"/>	ServerMigration_ServiceR...	AWS managed	Permissions to allow the AWS Server ...
<input type="checkbox"/>	ServerMigrationConnector	AWS managed	Permissions to allow the AWS Server ...
<input type="checkbox"/>	ServerMigrationServiceCo...	AWS managed	Required permissions to use all featur...
<input type="checkbox"/>	ServerMigrationServiceLa...	AWS managed	Permissions to allow the AWS Server ...
<input type="checkbox"/>	ServerMigrationServiceRo...	AWS managed	Permissions to allow the AWS SMS to r...
<input type="checkbox"/>	ServiceQuotasFullAccess	AWS managed	Provides full access to Service Quotas
<input type="checkbox"/>	ServiceQuotasReadOnlyA...	AWS managed	Provides read only access to Service Q...
<input type="checkbox"/>	SimpleWorkflowFullAccess	AWS managed	Provides full access to the Simple Wor...
<input checked="" type="checkbox"/>	SupportUser	AWS managed - job function	This policy grants permissions to troub...
<input type="checkbox"/>	SystemAdministrator	AWS managed - job function	Grants full access permissions necessa...

► Set permissions boundary - optional

Cancel Previous Next

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences ENG IN 14:47 09-02-2024

us-east-1.console.aws.amazon.com/iam/home?region=eu-north-1#/roles/create?trustedEntityType=CUSTOM\_TRUST\_POLICY&policies=arn%3Aaws%3Aiam%3A%

Step 2  
Add permissions

Step 3  
Name, review, and create

Role details

Role name  
SupportUserRole

Description  
They offer full fledged support to the user and help others to take the reference.

Step 1: Select trusted entities

Trust policy

```
1 - {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Sid": "Statement1",
6       "Effect": "Allow",
7       "Action": "sts:AssumeRole",
8       "Principal": "arn:aws:iam::123456789012:root"
9     }
10  ]
11 }
```

CloudShell Feedback 25°C Haze © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences ENG IN 14:49 09-02-2024

us-east-1.console.aws.amazon.com/iam/home?region=eu-north-1#/roles

Identity and Access Management (IAM)

Roles (3) Info

An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.

View role Create role

Role name Trusted entities Last activity

Roles Anywhere Info

Authenticate your non AWS workloads and securely provide access to AWS services.

Manage

Access AWS from your non AWS workloads

Operate your non AWS workloads using the same authentication and authorization strategy that you use within AWS.

X.509 Standard

Use your own existing PKI infrastructure or use AWS Certificate Manager Private Certificate Authority to authenticate identities.

Temporary credentials

Use temporary credentials with ease and benefit from the enhanced security they provide.

CloudShell Feedback 25°C Haze © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences ENG IN 14:50 09-02-2024

us-east-1.console.aws.amazon.com/iam/home?region=eu-north-1#/roles/details/SupportUserRole?section=permissions

Identity and Access Management (IAM)

SupportUserRole Switch role link copied

They offer full fledged support to the user and help others to take the reference.

**Summary**

Creation date February 09, 2024, 14:50 (UTC+05:30)	ARN arn:aws:iam::590183748698:role/SupportUserRole
Last activity -	Maximum session duration 1 hour

**Permissions** **Trust relationships** **Tags** **Access Advisor** **Revoke sessions**

**Permissions policies (1) Info**

**CloudShell Feedback** © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences ENG IN 14:51 09-02-2024

us-east-1.console.aws.amazon.com/iam/home?region=eu-north-1#/policies/create

IAM > Policies > Create policy

Step 1 Specify permissions

Step 2 Review and create

**Specify permissions** Info

Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.

**Policy editor**

**Select a service**  
Specify what actions can be performed on specific resources in a service.

Service

**Actions** Visual JSON Actions ▾

- Import policy
- Generate CloudFormation template
- Optimize for readability
- Optimize for size

**+ Add more permissions**

Cancel Next

**CloudShell Feedback** © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences ENG IN 14:55 09-02-2024

us-east-1.console.aws.amazon.com/iam/home?region=eu-north-1#/policies/create

to create new cognito resources.

Step 1  
Specify permissions

Step 2  
Review and create

<input type="radio"/> AmazonEC2ContainerRegistryPowerUser	None	Provides full access to Amazon EC2 Container Registry repositories, but does not allow repository deletion or policy changes.
<input type="radio"/> AmazonElasticContainerRegistryPublicPowerUser	None	Provides full access to Amazon ECR Public repositories, but does not allow repository deletion or policy changes.
<input type="radio"/> AWSCodeCommitPowerUser	None	Provides full access to AWS CodeCommit repositories, but does not allow repository deletion.
<input type="radio"/> AWSDataPipeline_PowerUser	None	Provides full access to Data Pipeline, list access for S3, DynamoDB, Redshift, RDS, SNS, and IAM roles, and passRole access for default Roles.
<input type="radio"/> AWSKeyManagementServicePowerUser	None	Provides access to AWS Key Management Service (KMS).
<input checked="" type="radio"/> PowerUserAccess	None	Provides full access to AWS services and resources, but does not allow management of Users and groups.

Cancel Import policy

CloudShell Feedback

25°C Haze

Actions Global saloni786

ON editor

Cancel Next

Privacy Terms Cookie preferences ENG IN 14:56 09-02-2024

us-east-1.console.aws.amazon.com/iam/home?region=eu-north-1#/policies/create

Step 1  
Specify permissions

Step 2  
Review and create

### Review and create Info

Review the permissions, specify details, and tags.

#### Policy details

Policy name  
Enter a meaningful name to identify this policy.

Description - optional  
Add a short explanation for this policy.

Permissions defined in this policy Info

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences ENG IN 15:01 09-02-2024

The screenshot shows the AWS IAM Policies page. A green success message at the top states: "Policy PowerUserExamplePolicy created." The main area displays a table titled "Policies" with one row. The row contains the policy name "PowerUserExamplePolicy", its type "AWS Lambda", "Used as" "Lambda function", and a "Description" column which is currently empty. The table includes a search bar, a "Filter by Type" dropdown set to "All types", and a pagination bar showing pages 1 through 59.

## TASK 2:

### Grant access to the billing console

The screenshot shows the AWS Billing console. A blue info message at the top left says: "Introducing the new AWS account page experience. We've redesigned the AWS account page. Let us know what you think." A green success message below it says: "Your IAM Access setting was updated successfully." It includes a note: "by NWCD, you will need to create a separate Amazon Web Services China Account. [Learn more.](#)" The main content area shows "IAM user and role access to Billing information" with an "Edit" button. Below it, under "Reserved instance marketplace settings", there is a note about managing seller and bank account information.

us-east-1.console.aws.amazon.com/iam/home#/users/create

Services Search [Alt+S]

Step 2 Set permissions

Step 3 Review and create

Step 4 Retrieve password

### User details

User name: pcandella

The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = . @ \_ - (hyphen)

Provide user access to the AWS Management Console - *optional*  
If you're providing console access to a person, it's a best practice [to manage their access in IAM Identity Center](#).

**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.

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences Nifty bank +1.43% ENG IN 15:10 09-02-2024

us-east-1.console.aws.amazon.com/iam/home#/users/create

Services Search [Alt+S]

IAM > Users > Create user

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.

#### User groups (1)

Create group

Group name	Attached policies	Created
Users		

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences Nifty bank +1.43% ENG IN 15:10 09-02-2024

us-east-1.console.aws.amazon.com/iam/home#/users/create

BillingGroup user group created.

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 (2)**

Group name	Users	Attached policies	Created
BillingGroup	0	Billing	2024-02-09 (Now)
EmergencyAccessGroup	1	AdministratorAccess	2024-02-09 (38 min...)

Set permissions boundary - optional

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences 15:12 ENG IN 09-02-2024

us-east-1.console.aws.amazon.com/iam/home#/users/create

User created successfully

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

View user

Step 1 Specify user details

Step 2 Set permissions

Step 3 Review and create

Step 4 Retrieve password

**Retrieve 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://590183748698.signin.aws.amazon.com/console>

User name  pcandella

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 15:13 ENG IN 09-02-2024

us-east-1.console.aws.amazon.com/iam/home#/users/create

IAM > Users > Create user

Step 1 Specify user details

User details

User name: twhitlock

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.

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences ENG IN 15:15 09-02-2024

us-east-1.console.aws.amazon.com/iam/home#/users/create

IAM > Users > Create user

Step 1 Specify user details

User group name: SupportGroup

Permissions policies (1/913)

Filter by Type: supportuser

Policy name: SupportUser

Create user group

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences ENG IN 15:16 09-02-2024

us-east-1.console.aws.amazon.com/iam/home#/users/create

**SupportGroup user group created.**

IAM > Users > Create user

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.

#### User groups (3)

[Create group](#)

CloudShell Feedback 29°C Haze © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences ENG IN 15:16 09-02-2024

us-east-1.console.aws.amazon.com/iam/home#/users/create

**User created successfully**

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

View user

Step 1  
Specify user details

Step 2  
Set permissions

Step 3  
Review and create

Step 4  
Retrieve password

### Retrieve 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

Email sign-in instructions

Console sign-in URL  
<https://590183748698.signin.aws.amazon.com/console>

User name  
twhitlock

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

Cancel Download .csv file Return to users list

CloudShell Feedback 29°C Haze © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences ENG IN 15:17 09-02-2024

Screenshot of the AWS IAM User Details page for user 'twhitlock'.

**Summary**

ARN copied

Console access: Enabled without MFA

Created: February 09, 2024, 15:17 (UTC+05:30)

Last console sign-in: Never

Access key 1: Create access key

**Permissions** (1) Groups (1) Tags Security credentials Access Advisor

**Permissions policies (1)**

Permissions are defined by policies attached to the user directly or through groups.

Filter by Type: All types

Policy name: Type: Attached via

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences 15:19 09-02-2024 ENG IN

Screenshot of the 'Add principal' dialog box.

**Add principal**

Specify the principal type and ARN to add for the selected service.

Principal type: IAM Roles

ARN: arn:aws:iam::590183748698:user/twhitlock

Cancel Add principal

Preview external access

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences 15:20 09-02-2024 ENG IN

Custom trust policy

Create a custom trust policy to enable others to perform actions in this account.

```
1▼ {
2    "Version": "2012-10-17",
3    "Statement": [
4        {
5            "Sid": "Statement1",
6            "Effect": "Allow",
7            "Principal": [
8                "AWS": "arn:aws:iam::590183748698:user/twhitlock"
9            ],
10           "Action": "sts:AssumeRole"
11       }
12   ]
13 }
```

Edit statement Statement1 Remove

Add actions for STS

Filter actions

GetSessionToken Info

Access level - read or write

AssumeRole Info

AssumeRoleWithSAML Info

AssumeRoleWithWebIdentity Info

DecodeAuthorizationMessage Info

SetContext Info

SetSourceIdentity Info

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences ENG IN 15:20 09-02-2024

us-east-1.console.aws.amazon.com/iam/home#/roles/create?trustedEntityType=CUSTOM\_TRUST\_POLICY

IAM > Roles > Create role

Step 1 Select trusted entity

Step 2 Add permissions

Step 3 Name, review, and create

### Add permissions Info

Permissions policies (1/911) Info

Choose one or more policies to attach to your new role.

Filter by Type

Billing All types 4 matches

Policy name	Type	Description
AWSBillingConductorFull...	AWS managed	Use the AWSBillingConductorFullAccess...
AWSBillingConductorRea...	AWS managed	Use the AWSBillingConductorReadOnl...
AWSBillingReadOnlyAccess	AWS managed	Allows users to view bills on the Billing...
<b>Billing</b>	AWS managed - job function	Grants permissions for billing and cost...

► Set permissions boundary - optional

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences ENG IN 15:21 09-02-2024

us-east-1.console.aws.amazon.com/iam/home#/roles/create?trustedEntityType=CUSTOM\_TRUST\_POLICY&policies=arn%3aws%3iam%3A%3aws%3Apolicy%2...

IAM Services Search [Alt+S]

Step 1 Select trusted entity

Step 2 Add permissions

Step 3 Name, review, and create

## Name, review, and create

**Role details**

**Role name**  
Enter a meaningful name to identify this role.

Maximum 64 characters. Use alphanumeric and '+=\_.,@-\_.' characters.

**Description**  
Add a short explanation for this role.

Maximum 1000 characters. Use alphanumeric and '+=\_.,@-\_.' characters.

**Step 1: Select trusted entities** Edit

**Trust policy**

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

CloudShell Feedback ENG IN 15:22 09-02-2024

us-east-1.console.aws.amazon.com/iam/home#/roles

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

- User groups
- Users
- Roles**
- Policies
- Identity providers
- Account settings

Access reports

- Access Analyzer
- External access
- Unused access

CloudShell Feedback ENG IN 15:22 09-02-2024

**Role TempBillingAccess created.**

**Roles (4) Info**View role Delete Create role

An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.

**Role name**

**Roles Anywhere** Info Manage

Authenticate your non AWS workloads and securely provide access to AWS services.

**Access AWS from your non AWS workloads**

Operate your non AWS workloads using the same authentication and authorization strategy that you use within AWS.

**X.509 Standard**

Use your own existing PKI infrastructure or use [AWS Certificate Manager Private Certificate Authority](#) to authenticate identities.

**Temporary credentials**

Use temporary credentials with ease and benefit from the enhanced security they provide.

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

## Delegate access across AWS accounts using roles

The image shows two screenshots of the AWS Management Console.

**AWS Support Center Screenshot:**

- URL: support.console.aws.amazon.com/support/home?region=us-east-1#/
- Account number: 381492030836
- Support plan: Basic Change
- Search bar: Search by service, errors, and more
- Quick solutions section:
  - Account & billing (selected)
  - Technical
- Topic list:
  - Billing (selected)
  - Account
  - Account Management
  - Free Tier
  - Getting Started
  - Education
- Top articles:
  - Learn what to do when your Free Tier period expires
  - Allow an IAM user to view my account's billing information
  - Learn about the AWS Free Tier
  - Managing your costs with AWS Budgets
  - Creating a billing alarm to monitor your estimated AWS charges
- Compute Optimizer panel:
  - Get recommendations to reduce the cost of your resources, or improve their performance. [Learn more.](#)
  - Enable Compute Optimizer
- Active cases and Create case buttons.

**IAM Policy Creation Screenshot:**

- URL: us-east-1.console.aws.amazon.com/iam/home#/policies/create
- Step 1: Specify permissions
- Step 2: Review and create
- Policy editor (JSON view):

```
1  {
2    "Version": "2012-10-17",
3    "Statement": [
4      {
5        "Effect": "Allow",
6        "Action": "s3:listAllMyBuckets",
7        "Resource": "*"
8      },
9      {
10        "Effect": "Allow",
11        "Action": [
12          "s3:ListBucket",
13          "s3:GetBucketLocation"
14        ],
15        "Resource": "arn:aws:s3:::productionapp"
16      },
17      {
18        "Effect": "Allow",
19        "Action": [
20          "s3:GetObject",
21          "s3:PutObject"
22        ],
23        "Resource": "arn:aws:s3:::productionapp/*"
24      }
25    ]
26  }
```
- Visual tab (selected)
- Actions tab
- Edit statement button
- Select a statement panel:
  - Select an existing statement in the policy or add a new statement.
  - + Add new statement
- © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

**Policy read-write-app-bucket created.**

**Identity and Access Management (IAM)**

**Policies (1177) Info**

A policy is an object in AWS that defines permissions.

Policy name	Type	Used as	Description
AmazonAPIGatewayA...	AWS managed	None	Provides full access to create/edit/delete...
AmazonAPIGatewayIn...	AWS managed	None	Provides full access to invoke APIs in A...
AmazonAPIGatewayP...	AWS managed	None	Allows API Gateway to push logs to us...
AmazonAppFlowFullA...	AWS managed	None	Provides full access to Amazon AppFlo...
AmazonAppFlowRead...	AWS managed	None	Provides read only access to Amazon A...
AmazonAppStreamFu...	AWS managed	None	Provides full access to Amazon AppStr...
AmazonAppStreamPC...	AWS managed	None	Amazon AppStream 2.0 access to AWS...
AmazonAppStreamRe...	AWS managed	None	Provides read only access to Amazon A...
AmazonAppStreamSe...	AWS managed	None	Default policy for Amazon AppStream ...

**Create role**

**Select trusted entity**

**Trusted entity type**

- AWS service Allow AWS services like EC2, Lambda, or others to perform actions in this account.
- AWS account Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.
- Web identity Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.

**An AWS account**

Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.

- This account (381492030836)
- Another AWS account

us-east-1.console.aws.amazon.com/iam/home#/roles/create?trustedEntityType=AWS\_ACCOUNT&policies=arn%3aws%3iam%3A%3A381492030836%3Apolicy%2Fread-write-app-bucket

Gmail YouTube Maps Translate New Tab Juniper Networks In... Cisco Skills For All Palo alto cyber All Bookmarks Global saloni786

IAM Services Search [Alt+S]

Step 1 Select trusted entity

Step 2 Add permissions

Step 3 Name, review, and create

## Name, review, and create

**Role details**

**Role name**  
Enter a meaningful name to identify this role.

Maximum 64 characters. Use alphanumeric and '+,-\_,@-' characters.

**Description**  
Add a short explanation for this role.

Maximum 1000 characters. Use alphanumeric and '+,-\_,@-' characters.

**Step 1: Select trusted entities**

**Trust policy**

```
1 - []
2 - "version": "2012-10-17",
```

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

CloudShell Feedback

us-east-1.console.aws.amazon.com/iam/home#/roles

Gmail YouTube Maps Translate New Tab Juniper Networks In... Cisco Skills For All Palo alto cyber All Bookmarks Global saloni786

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

- User groups
- Users
- Roles**
- Policies
- Identity providers
- Account settings

Access reports

- Access Analyzer
- External access
- Unused access
- Analyzer settings

Credential report

View role

Role UpdateApp created.

**Roles (7) Info**

An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.

Role name	Trusted entities	Last activity
UpdateApp	Account: 381492030836	-

**Roles Anywhere Info**

Authenticate your non AWS workloads and securely provide access to AWS services.

**Access AWS from your non AWS workloads**

Operate your non AWS workloads using the same authentication and authorization strategy that you use within AWS.

**X.509 Standard**

Use your own existing PKI infrastructure or use AWS Certificate Manager Private Certificate Authority to authenticate identities.

**Temporary credentials**

Use temporary credentials with ease and benefit from the enhanced security they provide.

CloudShell Feedback

us-east-1.console.aws.amazon.com/iam/home#/groups/details/SupportGroup/createPolicy

Gmail YouTube Maps Translate New Tab Juniper Networks Inc. Cisco Skills For All Palo alto cyber

All Bookmarks

IAM Services Search [Alt+S]

IAM > User groups > SupportGroup > Create policy

Step 1 Specify permissions Step 2 Review and create

Specify permissions Info

Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.

Policy editor

```
1 {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {"Effect": "Allow",  
5      "Action": "sts:AssumeRole",  
6      "Resource": "arn:aws:iam::381492030836:role/UpdateApp"  
7    }  
8  ]
```

Visual JSON Actions ▾

Edit statement

Select a statement

Select an existing statement in the policy or add a new statement.

+ Add new statement

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

Identity and Access Management (IAM)

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

Policy allow-assume-S3-role-in-production created.

IAM > User groups > SupportGroup

SupportGroup Info

Delete

Summary

Edit

User group name: SupportGroup Creation time: February 09, 2024, 15:16 (UTC+05:30) ARN: arn:aws:iam::381492030836:group/SupportGroup

Users (1) Permissions Access Advisor

Permissions policies (2) Info

You can attach up to 10 managed policies.

Filter by Type

Search Policy name Type Attached entities

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

## Create a customer managed policy

The screenshot shows two screenshots of the AWS IAM console. The top screenshot is the 'Specify permissions' step of the 'Create policy' wizard. It displays a JSON editor with the following code:

```
1 Version: "2012-10-17",
2 Statement: [
3     {
4         Effect: "Allow",
5         Action: [
6             "iam:GenerateCredentialReport",
7             "iam:Get*",
8             "iam>List*"
9         ],
10        Resource: "*"
11    }
12 ]
```

The bottom screenshot shows the 'Policies' list page. A green banner at the top indicates that a policy has been created: 'Policy UsersReadOnlyAccessToIAMConsole created.' The table lists various AWS managed policies:| Policy name | Type | Used as | Description |
| --- | --- | --- | --- |
| AmazonAPIGatewayAllActions | AWS managed | None | Provides full access to create/edit/delete API Gateway resources. |
| AmazonAPIGatewayInvokeFull | AWS managed | None | Provides full access to invoke APIs in Amazon API Gateway. |
| AmazonAPIGatewayPushToCloudWatchLogs | AWS managed | None | Allows API Gateway to push logs to CloudWatch Logs. |
| AmazonAppFlowFullAccess | AWS managed | None | Provides full access to Amazon AppFlow. |
| AmazonAppFlowReadOnlyAccess | AWS managed | None | Provides read only access to Amazon AppFlow. |
| AmazonAppStreamFullAccess | AWS managed | None | Provides full access to Amazon AppStream 2.0. |
| AmazonAppStreamPCAccess | AWS managed | None | Amazon AppStream 2.0 access to AWS Lambda functions. |
| AmazonAppStreamReadOnlyAccess | AWS managed | None | Provides read only access to Amazon AppStream 2.0. |
| AmazonAppStreamServiceAccess | AWS managed | None | Default policy for Amazon AppStream 2.0. |

**Conclusion :** Through this practical, we learnt to configure AWS Identity and Management (IAM) Console.

