

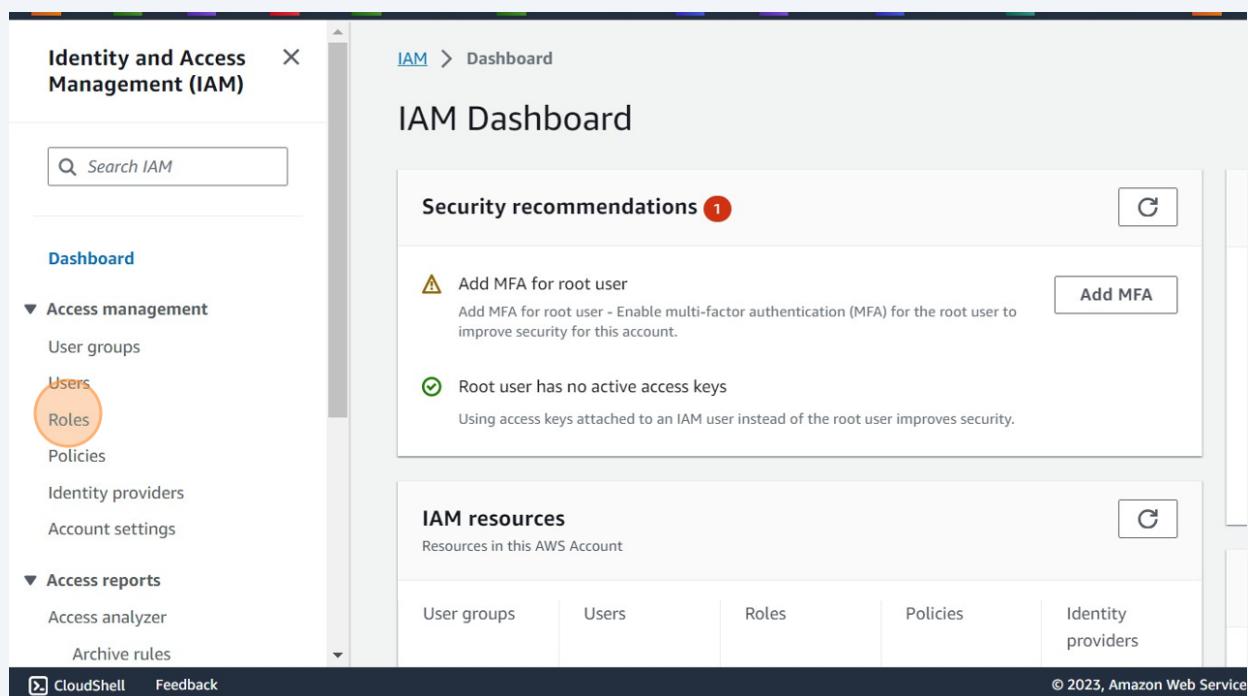
Create an IAM Role for EC2 in AWS Console

This guide provides step-by-step instructions on how to create an IAM role for EC2 in the AWS Console. By following this guide, users can easily set up the necessary permissions and access controls for their EC2 instances, ensuring secure and efficient management of their resources.

This guide was created by Nijat Hajiyev

- 1 Navigate to aws.amazon.com

- 2 Click "Roles"



3 Click "Create role"

The screenshot shows the AWS Identity and Access Management (IAM) service. On the left, there's a sidebar with options like Dashboard, Access management, Roles (which is selected), Policies, Identity providers, Account settings, Access reports, and Access analyzer. The main area is titled 'Roles (34) Info' and contains a table of roles. The 'Create role' button is highlighted with a red circle. The table includes columns for Role name, Trusted entities, and AWS Service.

Role name	Trusted entities	AWS Service
AmazonSageMaker-ExecutionRole-20230803T215540		sage
AmazonSageMaker-ExecutionRole-20231005T133540		sage
AmazonSagemakerCanvasForecastRole-20231005T133539		for
AmazonSagemakerCanvasForecastRole-sagemakerprofile		for
AmazonSageMakerServiceCatalogProductsApiGatewayRole		api
AmazonSageMakerServiceCatalogProductsCloudformationRole		clo

4 Click "AWS service"

The screenshot shows the 'Create role' wizard at Step 1: 'Select trusted entity'. The left sidebar lists steps: Step 1 (Select trusted entity), Step 2 (Add permissions), and Step 3 (Name, review, and create). The main area is titled 'Select trusted entity' and shows a 'Trusted entity type' section. The 'AWS service' option is highlighted with a red circle. Other options include 'AWS account', 'Web identity', 'SAML 2.0 federation', and 'Custom trust policy'.

Trusted entity type
<input checked="" type="radio"/> AWS service Allow AWS services like EC2, Lambda, or others to perform actions in this account.
<input type="radio"/> AWS account Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.
<input type="radio"/> Web identity Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.
<input type="radio"/> SAML 2.0 federation Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.
<input type="radio"/> Custom trust policy Create a custom trust policy to enable others to perform actions in this account.

5 Click "Choose a service or use case"

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

Allow users federated with SAML 2.0 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.

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

Service or use case

Choose a service or use case

Feedback

© 2023, Amazon Web Services, Inc.

6 Click "EC2"

EC2

aws | Services | Search [Alt+S]

EC2 S3 VPC IAM AWS Budgets AWS Cost Explorer RDS Route 53 DynamoDB Amazon SageMaker Lambda

Filter service or use case

Commonly used services

EC2

Lambda

Other services

Amazon EMR Serverless

Amazon OpenSearch Service

Amazon Grafana

Amplify

API Gateway

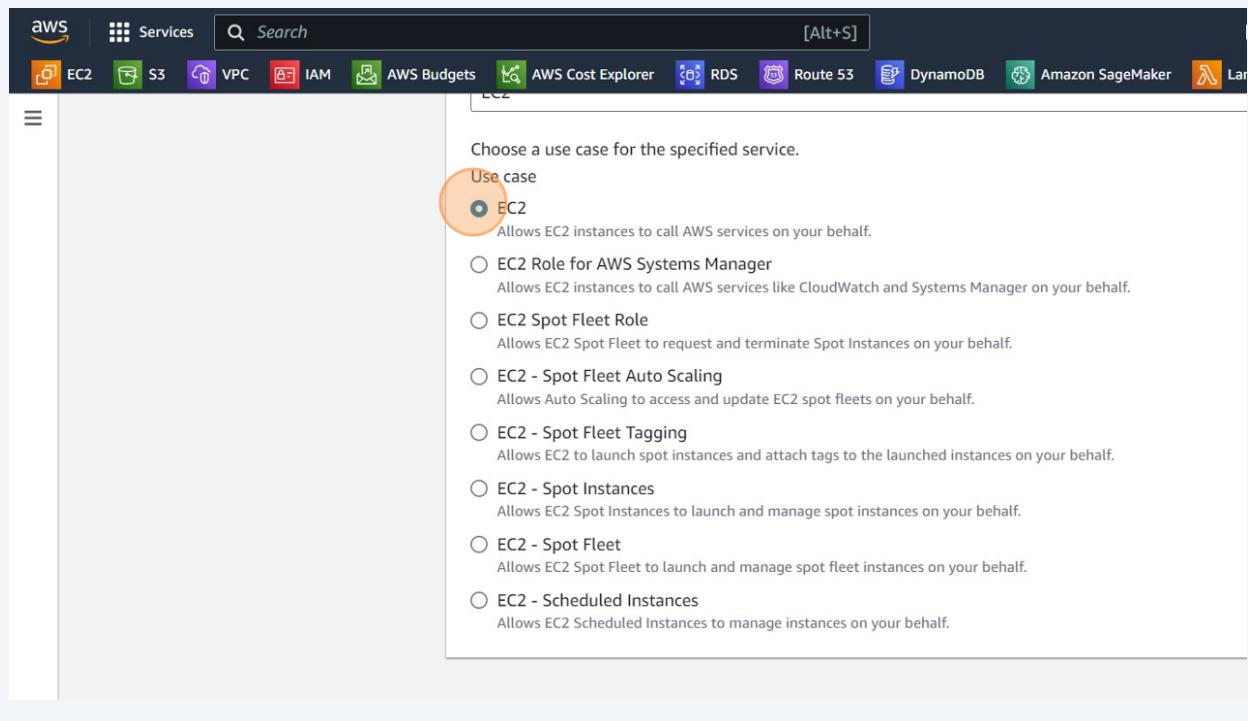
AppFabric

Application Auto Scaling

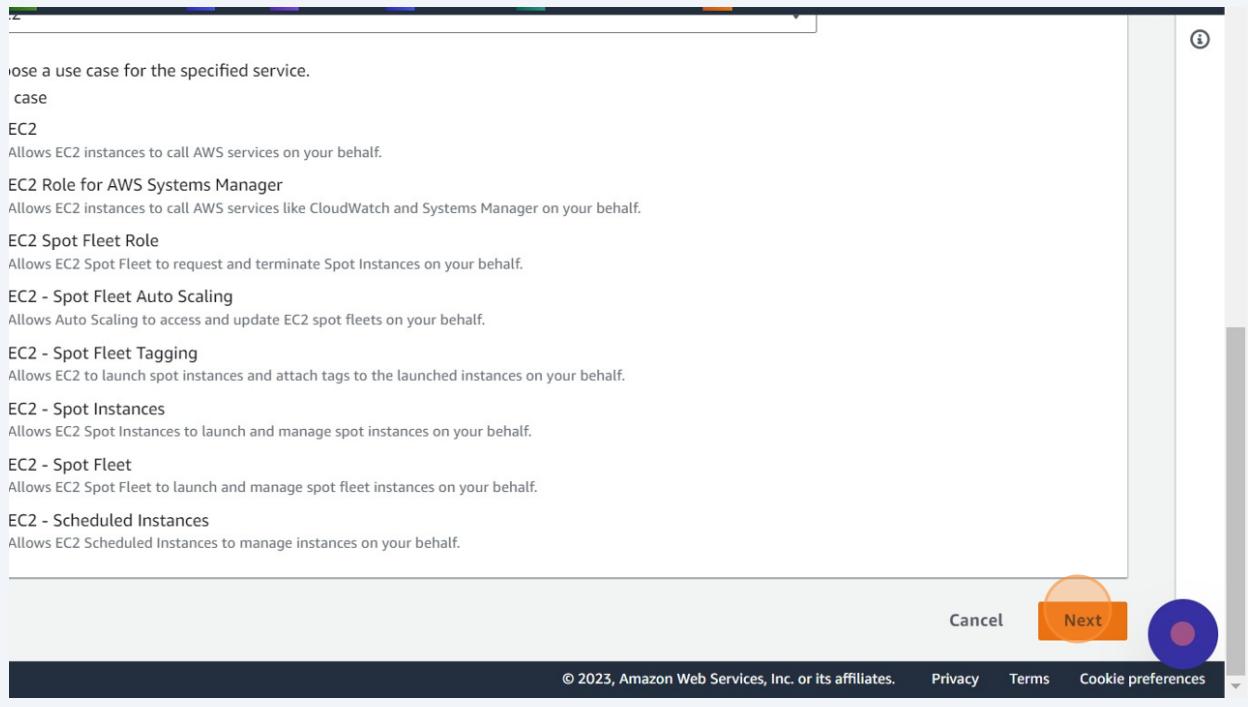
Application Discovery Service

Choose a service or use case

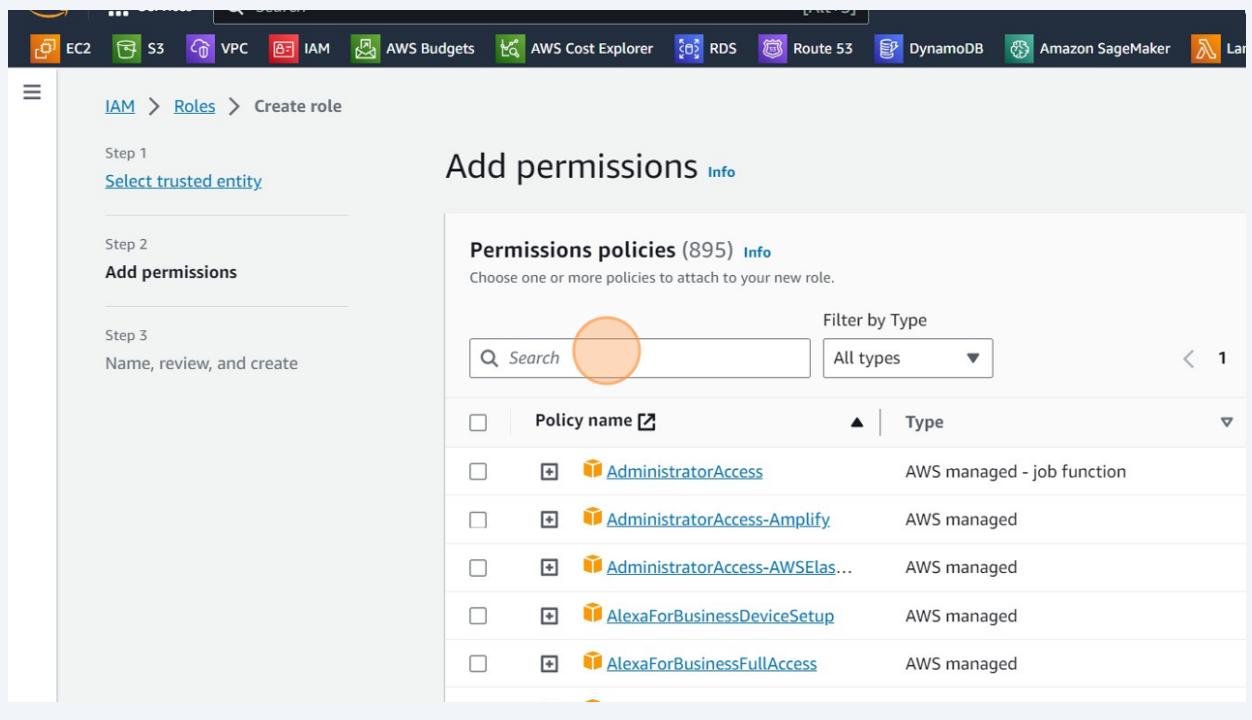
7 Click this radio button.



8 Click "Next"



9 Click the "Search" field.



The screenshot shows the AWS IAM 'Create role' wizard at Step 2: Add permissions. The left sidebar shows 'Step 1: Select trusted entity' and 'Step 3: Name, review, and create'. The main area is titled 'Add permissions' and shows a list of 'Permissions policies (895)'. A search bar is highlighted with an orange circle. The list includes several AWS managed policies:

Policy name	Type
AdministratorAccess	AWS managed - job function
AdministratorAccess-Amplify	AWS managed
AdministratorAccess-AWSElas...	AWS managed
AlexaForBusinessDeviceSetup	AWS managed
AlexaForBusinessFullAccess	AWS managed

10 Type "IAM"

11 Click this checkbox.

Screenshot of the AWS IAM 'Create role' wizard Step 2: Add permissions. The 'Permissions policies' section shows a list of AWS managed policies. The 'IAMFullAccess' policy is highlighted with an orange circle around its checkbox. The URL is [https://aws.amazon.com/console/home#/iam/roles/create-role?step=2®ion=us-east-1&roleName=MyTestRole&permissionsPolicySearchText=IAM](#).

Policy name	Type	Description
AWSQuickSightListIAM	AWS managed	Allow QuickSight to list IAM entities
IAMAccessAdvisorReadOnly	AWS managed	This policy grants access to read all acc...
IAMAccessAnalyzerFullAccess	AWS managed	Provides full access to IAM Access Anal...
IAMAccessAnalyzerReadOnlyA...	AWS managed	Provides read only access to IAM Acces...
IAMFullAccess	AWS managed	Provides full access to IAM via the AW...
IAMReadOnlyAccess	AWS managed	Provides read only access to IAM via th...
IAMSelfManageServiceSpecifi...	AWS managed	Allows an IAM user to manage their o...
IAMUserChangePassword	AWS managed	Provides the ability for an IAM user to ...
IAMUserSSHKeys	AWS managed	Provides the ability for an IAM user to ...

12 Click "Next"

Screenshot of the 'Set permissions boundary - optional' step. The 'IAMFullAccess' policy is selected in the previous step. The 'Next' button is highlighted with an orange circle. The URL is [https://aws.amazon.com/console/home#/iam/roles/create-role?step=3®ion=us-east-1&roleName=MyTestRole&permissionsPolicySearchText=IAM](#).

13 Click the "Role name" field.

The screenshot shows the AWS IAM Role Details page. At the top, there's a navigation bar with icons for VPC, IAM, AWS Budgets, AWS Cost Explorer, RDS, Route 53, DynamoDB, Amazon SageMaker, and Lambda. Below the navigation bar, the page title is "Role details". On the left, there's a sidebar with options like "View, and create" and "Sessions". The main content area has two fields: "Role name" and "Description". The "Role name" field is highlighted with a large orange circle. Below it, a note says "Maximum 64 characters. Use alphanumeric and '+-=.,@-_'" characters. The "Description" field contains the text "Allows EC2 instances to call AWS services on your behalf." Below it, a note says "Maximum 1000 characters. Use alphanumeric and '+-=.,@-_'" characters. At the bottom of the page, there's a section titled "Step 1: Select trusted entities".

14 Type "RoleforEC2"

15 Check "Step 1: Select trusted entities"

The screenshot shows the AWS IAM Trust Policy configuration page. At the top, there's a navigation bar with various services like EC2, S3, VPC, IAM, AWS Budgets, AWS Cost Explorer, RDS, Route 53, DynamoDB, Amazon SageMaker, and Lambda. Below the navigation bar, the title "Step 1: Select trusted entities" is highlighted with an orange circle. The main content area is titled "Trust policy" and contains the following JSON code:

```
1 {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {  
5       "Effect": "Allow",  
6       "Action": [  
7         "sts:AssumeRole"  
8       ],  
9       "Principal": {  
10         "Service": [  
11           "ec2.amazonaws.com"  
12         ]  
13     }  
14   ]  
15 }  
16 }
```

Below the trust policy, there are two sections: "Step 2: Add permissions" and "Permissions policy summary".

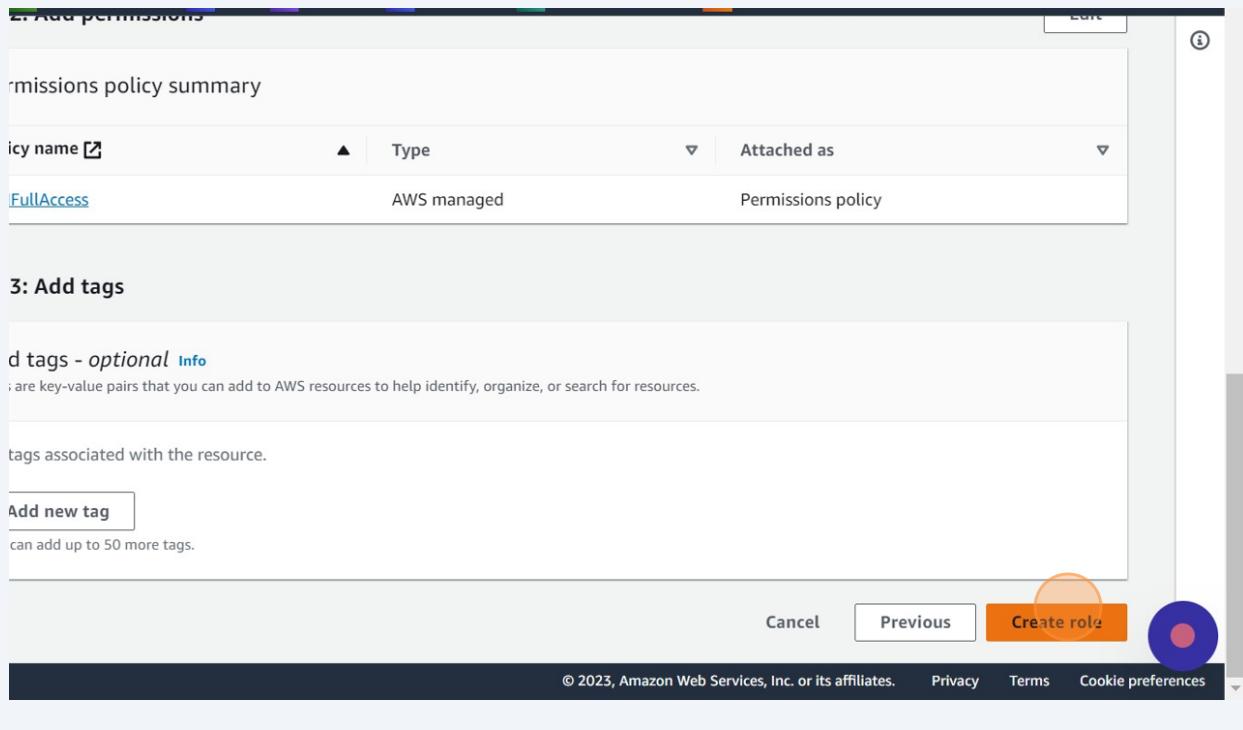
16 Check "Step 2: Add permissions"

The screenshot shows the AWS IAM Permissions Policy Summary page. At the top, there's a navigation bar with various services like EC2, S3, VPC, IAM, AWS Budgets, AWS Cost Explorer, RDS, Route 53, DynamoDB, and Lambda. Below the navigation bar, the title "Step 2: Add permissions" is highlighted with an orange circle. The main content area shows a table with one row:

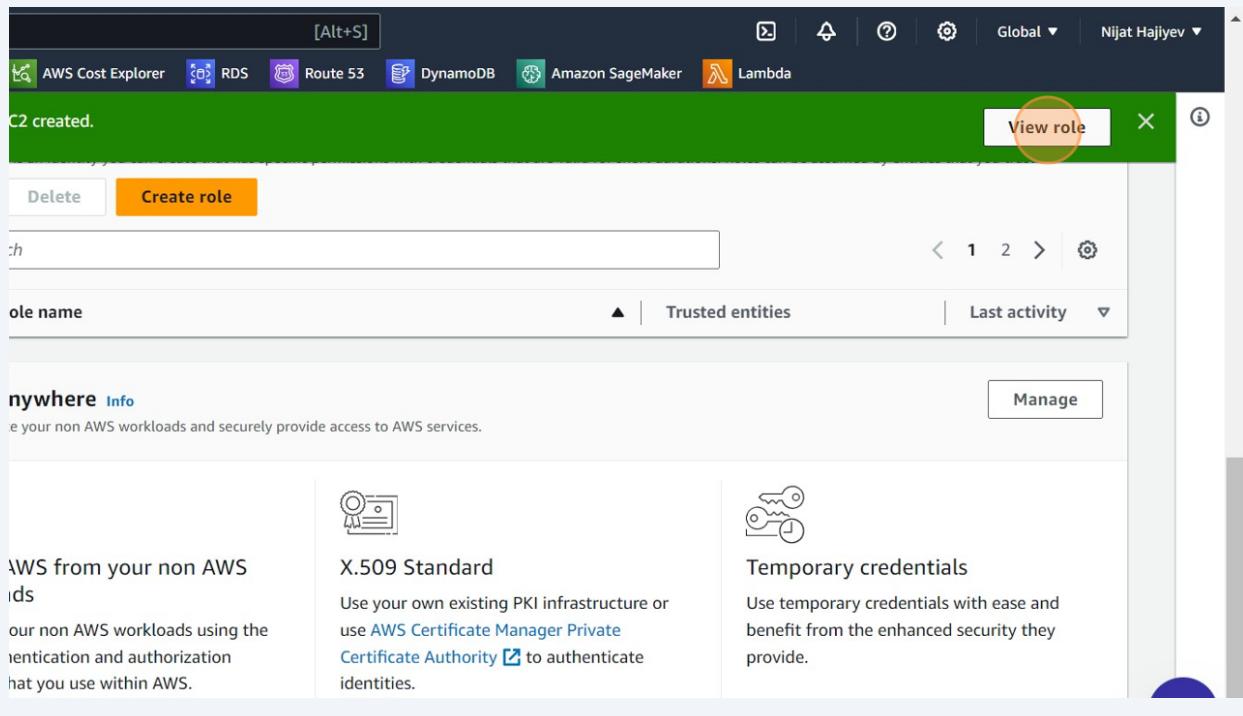
Policy name	Type
IAMFullAccess	AWS managed

Below the table, there's a section titled "Step 3: Add tags" with a sub-section "Add tags - optional". It includes a note: "Tags are key-value pairs that you can add to AWS resources to help identify, organize, or".

17 Click "Create role"



18 Click "View role"



19 Check "Permissions policies"

The screenshot shows the AWS IAM console. The left sidebar has sections for Access management (User groups, Users, Roles, Policies, Identity providers) and Access reports (Access analyzer, Archive rules). The main area is titled "Identity and Access Management (IAM)". It has tabs for Permissions, Trust relationships, Tags, and Access Advisor. The "Permissions" tab is selected. A section titled "Permissions policies (1)" is shown, with a note: "You can attach up to 10 managed policies." Below is a search bar and a table with one row: Policy name: IAMFullAccess, Type: AWS managed. The "IAMFullAccess" link is highlighted with an orange circle.

20 Check permission

This screenshot is similar to the previous one but includes additional UI elements. At the bottom of the main content area, there are two expandable sections: "Permissions boundary (not set)" and "Generate policy based on CloudTrail events". The "IAMFullAccess" policy row in the table has its checkbox selected, indicated by an orange circle around the checkbox icon.