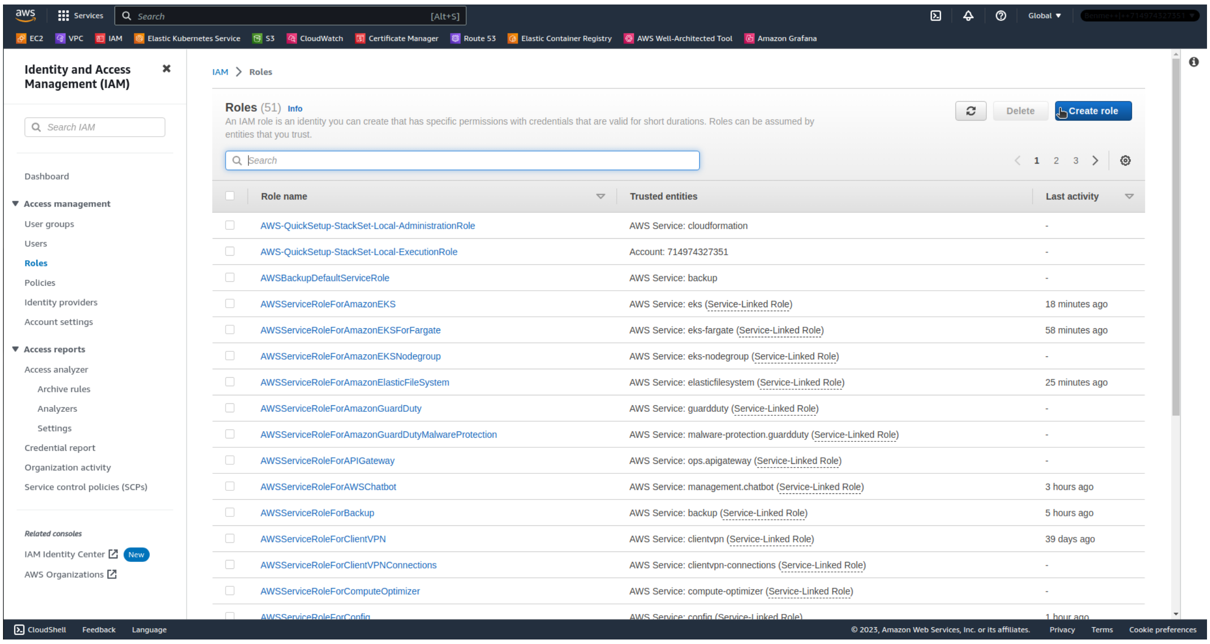
How to create IAM role for EKS service account

1. Open AWS Console and navigate to IAM service and head to “Roles”.

2. Next Click on “Create role” button in upper right.



Roles (51)

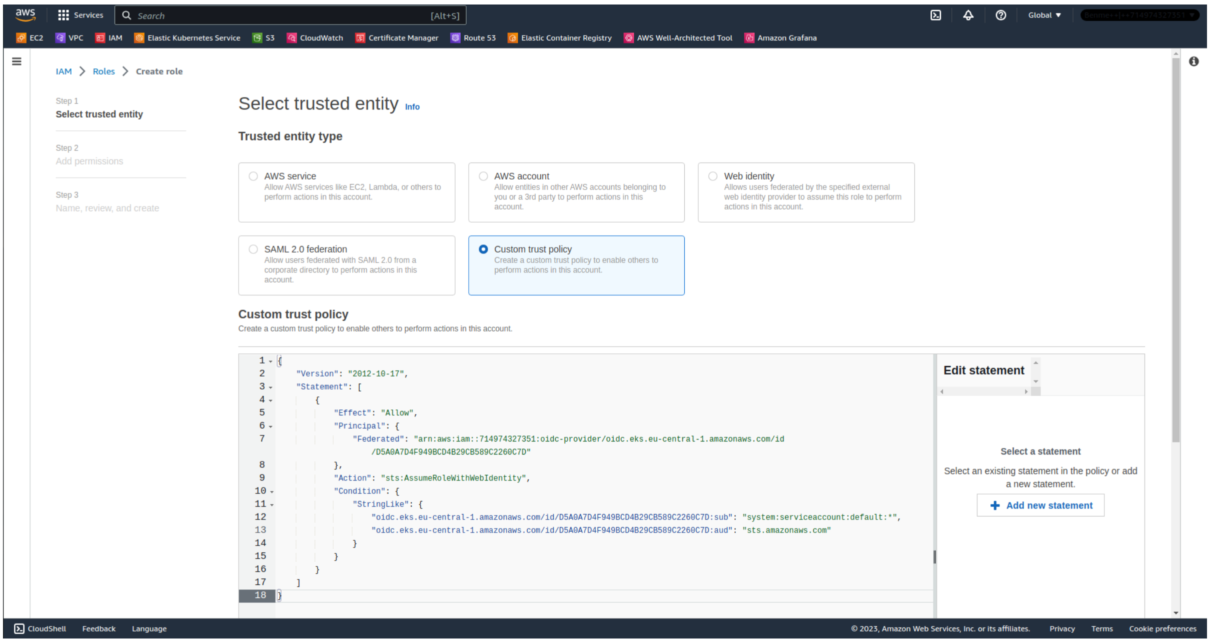
An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.

□	Role name	Trusted entities	Last activity
□	AWS-QuickSetup-StackSet-Local-AdministrationRole	AWS Service: cloudformation	-
□	AWS-QuickSetup-StackSet-Local-ExecutionRole	Account: 714974327351	-
□	AWSBackupDefaultServiceRole	AWS Service: backup	-
□	AWSServiceRoleForAmazonEKS	AWS Service: eks (Service-Linked Role)	18 minutes ago
□	AWSServiceRoleForAmazonEKSForFargate	AWS Service: eks-fargate (Service-Linked Role)	58 minutes ago
□	AWSServiceRoleForAmazonEKSNodegroup	AWS Service: eks-nodegroup (Service-Linked Role)	-
□	AWSServiceRoleForAmazonElasticFileSystem	AWS Service: elasticfilesystem (Service-Linked Role)	25 minutes ago
□	AWSServiceRoleForAmazonGuardDuty	AWS Service: guardduty (Service-Linked Role)	-
□	AWSServiceRoleForAmazonGuardDutyMalwareProtection	AWS Service: malware-protection.guardduty (Service-Linked Role)	-
□	AWSServiceRoleForAPIGateway	AWS Service: ops.apigateway (Service-Linked Role)	-
□	AWSServiceRoleForAWSChatbot	AWS Service: management.chatbot (Service-Linked Role)	3 hours ago
□	AWSServiceRoleForBackup	AWS Service: backup (Service-Linked Role)	5 hours ago
□	AWSServiceRoleForClientVPN	AWS Service: clientvpn (Service-Linked Role)	39 days ago
□	AWSServiceRoleForClientVPNConnections	AWS Service: clientvpn-connections (Service-Linked Role)	-
□	AWSServiceRoleForComputeOptimizer	AWS Service: compute-optimizer (Service-Linked Role)	-
□	AWSServiceRoleForConfig	AWS Service: config (Service-Linked Role)	1 hour ago

3. Select “Custom trust policy” and use policy as follows:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Federated": "arn:aws:iam::111122223333:oidc-provider/oidc.eks.region-code.amazonaws.com/id/EXAMPLED539D4633E53DE1B71EXAMPLE"
            },
            "Action": "sts:AssumeRoleWithWebIdentity",
            "Condition": {
                "StringLike": {
                    "oidc.eks.region-code.amazonaws.com/id/EXAMPLED539D4633E53DE1B71EXAMPLE:sub": "system:serviceaccount:*",
                    "oidc.eks.region-code.amazonaws.com/id/EXAMPLED539D4633E53DE1B71EXAMPLE:aud": "sts.amazonaws.com"
                }
            }
        }
    ]
}
```

You can get OIDC provider arn and name from IAM Service > [Identity providers](). Remember to change region-code. Values to change are marked blue.


aws
Services
Search
[Alt+S]
Global
EC2
VPC
IAM
Elastic Kubernetes Service
S3
CloudWatch
Certificate Manager
Route 53
Elastic Container Registry
AWS Well-Architected Tool
Amazon Grafana
IAM > Roles > Create role
Edit statement
Select a statement
Select an existing statement in the policy or add a new statement.
+ Add new statement
CloudShell
Feedback
Language
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

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.

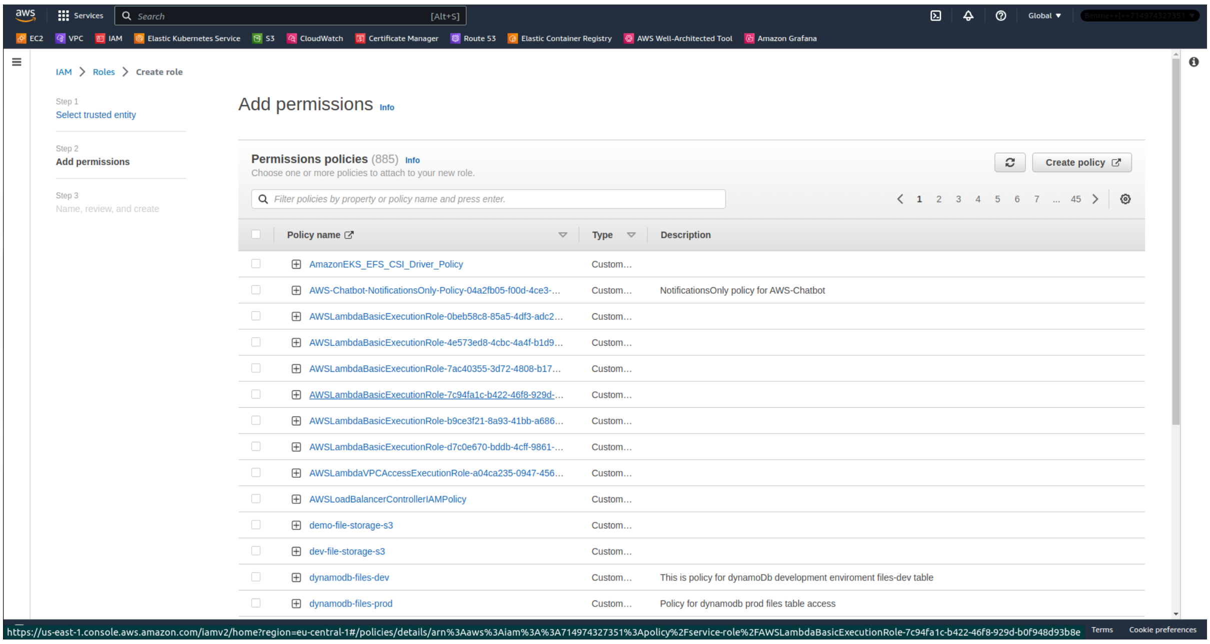
● Custom trust policy
Create a custom trust policy to enable others to perform actions in this account.

Custom trust policy

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

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Federated": "arn:aws:iam::714974327351:oidc-provider/oidc.eks.eu-central-1.amazonaws.com/id/D5A0A7D4F949BCD4B29CB589C2260C7D"
            },
            "Action": "sts:AssumeRoleWithWebIdentity",
            "Condition": {
                "StringLike": {
                    "oidc.eks.eu-central-1.amazonaws.com/id/D5A0A7D4F949BCD4B29CB589C2260C7D:sub": "system:serviceaccount:default:*",
                    "oidc.eks.eu-central-1.amazonaws.com/id/D5A0A7D4F949BCD4B29CB589C2260C7D:aud": "sts.amazonaws.com"
                }
            }
        }
    ]
}
```

4. Click on “Next” in the right bottom and add permissions to the IAM Role.



aws
Services
Search [Alt+S]
Global ▼
[redacted]
EC2 VPC IAM Elastic Kubernetes Service S3 CloudWatch Certificate Manager Route 53 Elastic Container Registry AWS Well-Architected Tool Amazon Grafana
IAM > Roles > Create role

Step 1
Select trusted entity

Step 2
Add permissions

Step 3
Name, review, and create

Add permissions Info

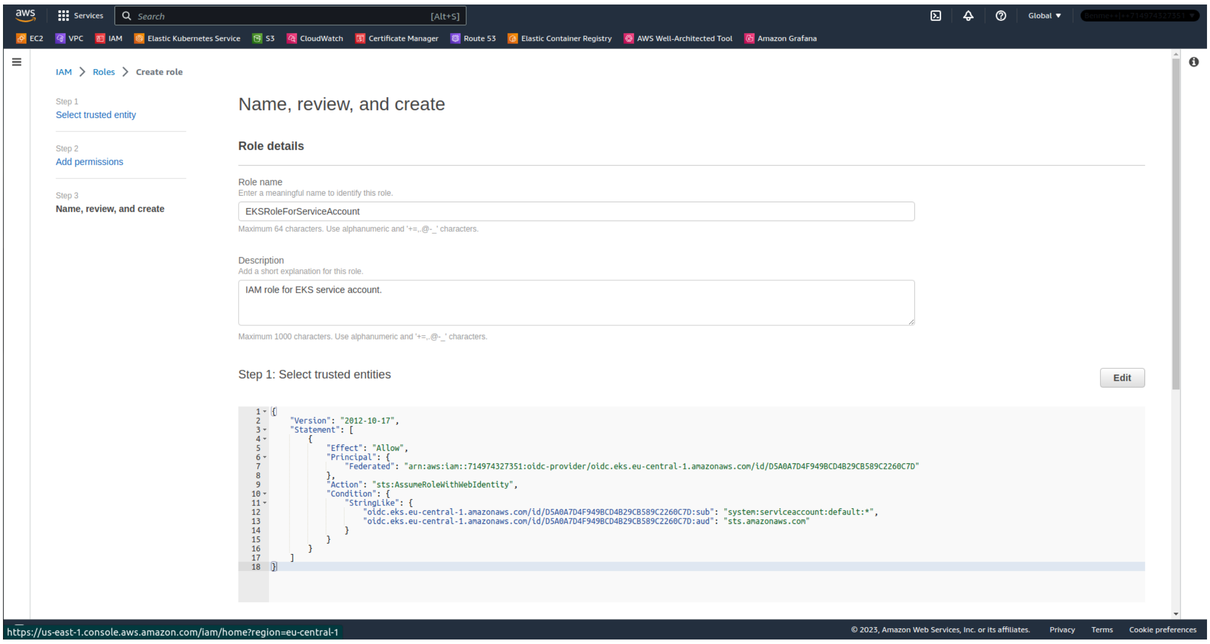
Permissions policies (885) Info
Choose one or more policies to attach to your new role.

Create policy
Filter policies by property or policy name and press enter.
< 1 2 3 4 5 6 7 ... 45 >

□	Policy name	Type	Description
□	⊞ AmazonEKS_EFS_CSI_Driver_Policy	Custom...	
□	⊞ AWS-Chatbot-NotificationsOnly-Policy-04a2fb05-f00d-4ce3-...	Custom...	NotificationsOnly policy for AWS-Chatbot
□	⊞ AWSLambdaBasicExecutionRole-0beb58c8-85a5-4df3-adc2...	Custom...	
□	⊞ AWSLambdaBasicExecutionRole-4e573ed8-4cbc-4a4f-b1d9...	Custom...	
□	⊞ AWSLambdaBasicExecutionRole-7ac40355-3d72-4808-b17...	Custom...	
□	⊞ AWSLambdaBasicExecutionRole-7c94fa1c-b422-46f8-929d-...	Custom...	
□	⊞ AWSLambdaBasicExecutionRole-b9ce3f21-8a93-41bb-a686...	Custom...	
□	⊞ AWSLambdaBasicExecutionRole-d7c0e670-bddb-4cff-9861-...	Custom...	
□	⊞ AWSLambdaVPCAccessExecutionRole-a04ca235-0947-456...	Custom...	
□	⊞ AWSLoadBalancerControllerIAMPolicy	Custom...	
□	⊞ demo-file-storage-s3	Custom...	
□	⊞ dev-file-storage-s3	Custom...	
□	⊞ dynamodb-files-dev	Custom...	This is policy for dynamoDb development enviroment files-dev table
□	⊞ dynamodb-files-prod	Custom...	Policy for dynamodb prod files table access

https://us-east-1.console.aws.amazon.com/iamv2/home?region=eu-central-1#/policies/details/arn%3Aaws%3Aiam%3A%3A714974327351%3Apolicy%2Fservice-role%2FAWSLambdaBasicExecutionRole-7c94fa1c-b422-46f8-929d-b0f948d93b8e

5. Give the Role a name, optionally description and click on “Create role” in the bottom right.



aws
Services
Search [Alt+S]
Global ▼
[redacted]
EC2 VPC IAM Elastic Kubernetes Service S3 CloudWatch Certificate Manager Route 53 Elastic Container Registry AWS Well-Architected Tool Amazon Grafana
IAM > Roles > Create role

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

Description
Add a short explanation for this role.
IAM role for EKS service account.
Maximum 1000 characters. Use alphanumeric and '+=,.@-_' characters.

Step 1: Select trusted entities

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Federated": "arn:aws:iam::714974327351:oidc-provider/oidc.eks.eu-central-1.amazonaws.com/id/D5A0A7D4F949BCD4B29CB589C2260C7D"
            },
            "Action": "sts:AssumeRoleWithWebIdentity",
            "Condition": {
                "StringLike": {
                    "oidc.eks.eu-central-1.amazonaws.com/id/D5A0A7D4F949BCD4B29CB589C2260C7D:sub": "system:serviceaccount:default:*",
                    "oidc.eks.eu-central-1.amazonaws.com/id/D5A0A7D4F949BCD4B29CB589C2260C7D:aud": "sts.amazonaws.com"
                }
            }
        }
    ]
}
```

https://us-east-1.console.aws.amazon.com/iam/home?region=eu-central-1

6. Now create Service Account in Kubernetes which will assume the role. Here’s the example manifest:

```
apiVersion: v1
kind: ServiceAccount
metadata:
  name: example-service-account
  namespace: default
  annotations:
    eks.amazonaws.com/role-arn: arn:aws:iam::714974327351:role/EKSRoleForServiceAccount
```