

Amazon EKS (WOW Factor)

1) Creating service role

The screenshot shows the AWS IAM Management Console with the URL [https://console.aws.amazon.com/iam/home#/roles\\$new?step=type](https://console.aws.amazon.com/iam/home#/roles$new?step=type). The page is titled "Create role" and displays the first step of the wizard: "Select type of trusted entity". There are four options: "AWS service" (selected), "Another AWS account", "Web identity", and "SAML 2.0 federation". Below the options, a note states: "Allows AWS services to perform actions on your behalf. [Learn more](#)". Step 1 is highlighted with a blue circle. Step 2 is the next button.

Select type of trusted entity

- AWS service** EC2, Lambda and others
- Another AWS account Belonging to you or 3rd party
- Web identity Cognito or any OpenID provider
- SAML 2.0 federation Your corporate directory

Allows AWS services to perform actions on your behalf. [Learn more](#)

Choose the service that will use this role

EC2
Allows EC2 instances to call AWS services on your behalf.

Lambda
Allows Lambda functions to call AWS services on your behalf.

API Gateway	CodeBuild	EC2 - Fleet	IoT	Redshift
AWS Support	CodeDeploy	EKS	Kinesis	Rekognition
Amplify	Config	EMR	Lambda	S3
AppSync	Connect	ElastiCache	Lex	SMS
Application Auto Scaling	DMS	Elastic Beanstalk	License Manager	SNS
Application Discovery Service	Data Lifecycle Manager	Elastic Container Service	Machine Learning	SWF
Auto Scaling	Data Pipeline	Elastic Transcoder	Macie	SageMaker
Batch	DataSync	Elastic Load Balancing	MediaConvert	Service Catalog
CloudFormation	DeepLens	Glue	OpsWorks	Step Functions
CloudHSM	Directory Service	Greengrass	RAM	Storage Gateway
CloudTrail	DynamoDB	GuardDuty	RDS	Trusted Advisor
CloudWatch Events	EC2	Inspector		

* Required [Cancel](#) [Next: Permissions](#)

© 2008 - 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved. [Privacy Policy](#) [Terms of Use](#)

<https://console.aws.amazon.com/iam/home#/roles/new?step=review&selectedService=AmazonEKS&selectedUseCase=AmazonEKS>

Create role

Review

Provide the required information below and review this role before you create it.

Role name* eksServiceRole_281
Use alphanumeric and '+=_,@-' characters. Maximum 64 characters.

Role description Allows EKS to manage clusters on your behalf.
Maximum 1000 characters. Use alphanumeric and '+=_,@-' characters.

Trusted entities AWS service: eks.amazonaws.com

Policies AmazonEKSClusterPolicy AmazonEKSServicePolicy

Permissions boundary Permissions boundary is not set

No tags were added.

* Required

[Feedback](#) [English \(US\)](#)

https://console.aws.amazon.com/iam/home#/roles/eksServiceRole_281

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

[Feedback](#) [English \(US\)](#)

[Search IAM](#)

[Dashboard](#) [Groups](#) [Users](#) [Roles](#) [Policies](#) [Identity providers](#) [Account settings](#) [Credential report](#) [Encryption keys](#)

[Roles > eksServiceRole_281](#)

Summary

Role ARN	arn:aws:iam::326071200148:role/eksServiceRole_281
Role description	Allows EKS to manage clusters on your behalf. Edit
Instance Profile ARNs	
Path	/
Creation time	2018-01-01 10:41 PST
Maximum CLI/API session duration	1 hour Edit

[Permissions](#) [Trust relationships](#) [Tags](#) [Access Advisor](#) [Revoke sessions](#)

[Attach policies](#) [Add inline policy](#)

Policy name	Policy type
AmazonEKSClusterPolicy	AWS managed policy
AmazonEKSServicePolicy	AWS managed policy

[Permissions boundary \(not set\)](#)

[Feedback](#) [English \(US\)](#)

© 2008 - 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved. [Privacy Policy](#) [Terms of Use](#)

2) Creating Policies for the role we created above

The screenshot shows the AWS IAM Management Console with the URL <https://console.aws.amazon.com/iam/home#/policies?new?step=edit>. The page title is "Create policy". A validation error message in a yellow box states: "This policy validation failed and might have errors converting to JSON : The policy must have at least one statement. For more information about the IAM policy grammar, see AWS IAM Policies". The JSON editor shows the following policy:

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

Buttons at the bottom include "Cancel" and "Review policy". The status bar at the bottom right indicates "© 2008 - 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use".

The screenshot shows the AWS IAM Management Console with the URL https://console.aws.amazon.com/iam/home#/policies/arn:aws:iam::326071200148:policy/AmazonEKSAdminPolicy_281/serviceLevelSummary. The left sidebar shows the "Policies" section selected. The main area displays the "Summary" for the "AmazonEKSAdminPolicy_281" policy. The policy ARN is arn:aws:iam::326071200148:policy/AmazonEKSAdminPolicy_281. The "Permissions" tab is selected, showing a table with one row for EKS with "Full access" and "All resources". Other tabs include "Policy usage", "Policy versions", and "Access Advisor". Buttons at the top right include "Delete policy" and a help icon. The status bar at the bottom right indicates "© 2008 - 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use".

The screenshot shows the AWS IAM Policy Summary page. The policy ARN is arn:aws:iam::326071200148:policy/AmazonEKSPassRole_281. The permissions table shows one entry:

Service	Access level	Resource	Request condition
IAM	Limited: Write	RoleName string like eksServiceRole_281	None

At the bottom, there are links for Feedback, English (US), Privacy Policy, and Terms of Use.

3) Attach policies to role

Add permissions to eksServiceRole_281

Attach Permissions

Create policy

Filter policies ▾

Policy name	Type	Used as	Description
AmazonEKS_CNI_Policy	AWS managed	None	This policy provides the Amazon VPC CNI Plugin (amazon-vpc-cni-k8s) the permissions it requires to ...
AmazonEKSAdminPolicy_281	Customer managed	None	
AmazonEKSPassRole_281	Customer managed	None	
AmazonEKSWorkerNodePolicy	AWS managed	None	This policy allows Amazon EKS worker nodes to connect to Amazon EKS Clusters.

Showing 4 results

Cancel **Attach policy**

Feedback English (US)

© 2008 - 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

Roles > eksServiceRole_281

Summary

2 policies have been attached for the eksServiceRole_281.

Role ARN: arn:aws:iam::326071200148:role/eksServiceRole_281

Role description: Allows EKS to manage clusters on your behalf. | Edit

Instance Profile ARNs:

Path: /

Creation time: 2018-12-01 10:41 PST

Maximum CLI/API session duration: 1 hour | Edit

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

▼ Permissions policies (4 policies applied)

Attach policies **Add inline policy**

Policy name	Policy type
AmazonEKSAdminPolicy_281	Managed policy
AmazonEKSClusterPolicy	AWS managed policy
AmazonEKSPassRole_281	Managed policy
AmazonEKSServicePolicy	AWS managed policy

▶ Permissions boundary (not set)

Feedback English (US)

© 2008 - 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

4) Creating a group for user

The screenshot shows the 'Create New Group Wizard' on the 'Review' step. The page title is 'Review'. It displays the following information:

- Group Name:** AWS_EKSGroup_281
- Policies:** am:aws:iam::aws:policy/AmazonEKSClusterPolicy, am:aws:iam::aws:policy/AmazonEKSWorkerNodePolicy, am:aws:iam::aws:policy/AmazonEKSServicePolicy, am:aws:iam::aws:policy/AmazonEKS_CNI_Policy, am:aws:iam::326071200148:policy/AmazonEKSAadminPolicy_281, am:aws:iam::326071200148:policy/AmazonEKSPassRole_281
- Edit Policies:** A link to edit the policies assigned to the group.

At the bottom right, there are 'Cancel', 'Previous', and 'Create Group' buttons.

The screenshot shows the 'Groups' section of the AWS IAM console. The left sidebar includes options like Dashboard, Groups (which is selected), Users, Roles, Policies, Identity providers, Account settings, Credential report, and Encryption keys. The main area displays a table of groups:

Group Name	Users	Inline Policy	Creation Time
AWSCloud9Group	1		2018-10-11 13:49 PST
<input checked="" type="checkbox"/> AWS_EKSGroup_281	0		2018-12-01 11:44 PST

At the bottom, there are 'Feedback', 'English (US)', and links to 'Privacy Policy' and 'Terms of Use'.

5) Creating a user

[https://console.aws.amazon.com/iam/home#/users\\$new?step=details](https://console.aws.amazon.com/iam/home#/users$new?step=details)

Add user

Set user details

You can add multiple users at once with the same access type and permissions. [Learn more](#)

User name* [Add another user](#)

Select AWS access type

Select how these users will access AWS. Access keys and autogenerated passwords are provided in the last step. [Learn more](#)

Access type* Programmatic access
Enables an access key ID and secret access key for the AWS API, CLI, SDK, and other development tools.

AWS Management Console access
Enables a password that allows users to sign-in to the AWS Management Console.

Console password* Autogenerated password
 Custom password

 Show password

Require password reset User must create a new password at next sign-in
Users automatically get the [IAMUserChangePassword](#) policy to allow them to change their own password.

* Required

[Cancel](#) [Next: Permissions](#)

[Feedback](#) [English \(US\)](#)

[https://console.aws.amazon.com/iam/home#/users\\$permissions&login&userNames=AWS_EKSUser_281&passwordReset&passwordType=manual](https://console.aws.amazon.com/iam/home#/users$permissions&login&userNames=AWS_EKSUser_281&passwordReset&passwordType=manual)

Add user

Set permissions

[Add user to group](#) [Copy permissions from existing user](#) [Attach existing policies directly](#)

Add user to group

[Create group](#) [Refresh](#)

Group	Attached policies
<input checked="" type="checkbox"/> AWS_EKSGroup_281	AmazonEKSAAdminPolicy_281 and 5 more
<input type="checkbox"/> AWSCloud9Group	AWSCloud9EnvironmentMember and 2 more

Set permissions boundary

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

[Feedback](#) [English \(US\)](#)

The screenshot shows the AWS IAM 'Add user' interface. At the top, there is a success message: "Success: You successfully created the users shown below. You can view and download user security credentials. You can also email users instructions for signing in to the AWS Management Console. This is the last time these credentials will be available to download. However, you can create new credentials at any time." Below this message, there is a table with one row containing the user 'AWS_EKSUser_281'. To the right of the table, there is a link 'Email login instructions' and a 'Send email' button. At the bottom of the page, there is a 'Download .csv' button.

6) Create a VPC cluster

The screenshot shows the AWS CloudFormation 'Create stack' wizard. The first step, 'Select Template', is selected. It displays a 'Design a template' section with a 'Design template' button and a 'Choose a template' section with three options: 'Select a sample template', 'Upload a template to Amazon S3', and 'Specify an Amazon S3 template URL'. The third option is selected, and the URL 'js-west-2.amazonaws.com/cloudformation/2018-11-07/amazon-eks-vpc-sample.yaml' is shown. At the bottom of the page, there are 'Cancel' and 'Next' buttons.

Create stack

Select Template
Specify Details
Options
Review

Review

Template

Template URL: <https://amazon-eks.s3-us-west-2.amazonaws.com/cloudformation/2018-11-07/amazon-eks-vpc-sample.yaml>
 Description: Amazon EKS Sample VPC
 Estimate cost: Cost

Details

Stack name: CMPE281-EKS-VPC

Worker Network Configuration

VpcBlock	192.168.0.0/16
Subnet01Block	192.168.64.0/18
Subnet02Block	192.168.128.0/18
Subnet03Block	192.168.192.0/18

Options

Tags

No tags provided

Rollback Triggers

No monitoring time provided

No rollback triggers provided

Advanced

Notification	Disabled
Termination Protection	Disabled
Timeout	none

Drift detection now available

Drift detection lets you detect whether a stack's actual configuration has been changed outside of CloudFormation. To detect drift on a stack, select the stack, and then select Detect drift for current stack from the Actions menu. Learn more.

Stack Name	Created Time	Status	Drift Status	Description
CMPE281-EKS-VPC	2018-12-01 12:15:45 UTC-0800	CREATE_COMPLETE	NOT_CHECKED	Amazon EKS Sample VPC

Event Log					
Date	Status	Type	Logical ID	Status Reason	
2018-12-01	CREATE_COMPLETE	AWS::CloudFormation::Stack	CMPE281-EKS-VPC		
2018-12-01	CREATE_COMPLETE	AWS::EC2::SubnetRouteTableAssociation	Subnet01RouteTableAssociatio	n	
2018-12-01	CREATE_COMPLETE	AWS::EC2::SubnetRouteTableAssociation	Subnet02RouteTableAssociatio	n	
2018-12-01	CREATE_COMPLETE	AWS::EC2::SubnetRouteTableAssociation	Subnet03RouteTableAssociatio	n	
2018-12-01	CREATE_COMPLETE	AWS::EC2::Route	Route		
2018-12-01	CREATE_IN_PROGRESS	AWS::EC2::SubnetRouteTableAssociation	Subnet01RouteTableAssociatio	Resource creation initiated	
2018-12-01	CREATE_IN_PROGRESS	AWS::EC2::SubnetRouteTableAssociation	Subnet02RouteTableAssociatio	Resource creation initiated	
2018-12-01	CREATE_IN_PROGRESS	AWS::EC2::SubnetRouteTableAssociation	Subnet03RouteTableAssociatio	n	

The redesigned AWS CloudFormation console is available now
We've completely redesigned the console to improve the overall look and feel. Try it out now and provide us feedback.

Drift detection now available
Drift detection lets you detect whether a stack's actual configuration has been changed outside of CloudFormation. To detect drift on a stack, select the stack, and then select Detect drift for current stack from the Actions menu. Learn more.

Stack Name	Created Time	Status	Drift Status	Description
CMPE281-EKS-VC	2018-12-01 12:15:45 UTC-0800	CREATE_COMPLETE	NOT_CHECKED	Amazon EKS Sample VPC

Outputs

Key	Value	Description	Export Name
SecurityGroups	sg-061411acb61b3ec60	Security group for the cluster control plane communication...	
VpcId	vpc-0e69bfbf33bf1046e	The VPC Id	
SubnetIds	subnet-061a96394001c00c0, subnet-09cfadc336abd9b3, subnet-088ec3226fbfc1684	All subnets in the VPC	

7) Create a AWS CLI for configuring users

```
Default region name [None]: us-west-2
Default output format [None]:
C02TH0ZVGTFM:Personal Project i869640$ aws configure
C02TH0ZVGTFM:Personal Project i869640$ aws eks create-cluster --name eksCluster --role-arn arn:aws:iam::326071200148:role/eksServiceRole_281 --resources=vpc-config subnetIds=subnet-061a96394001c00c0,subnet-09cfadc336abd9b3,subnet-088ec3226fbfc1684,securityGroupIds=sg-061411acb61b3ec60
[...]
{ must change your password.
  "cluster": {
    "name": "eksCluster",
    "arn": "arn:aws:eks:us-west-2:326071200148:cluster/eksCluster",
    "createdAt": 1543700693.297,
    "version": "1.10",
    "roleArn": "arn:aws:iam::326071200148:role/eksServiceRole_281",
    "resourcesVpcConfig": {
      "subnetIds": [
        "subnet-061a96394001c00c0",
        "subnet-09cfadc336abd9b3",
        "subnet-088ec3226fbfc1684"
      ],
      "securityGroupIds": [
        "sg-061411acb61b3ec60"
      ],
      "vpcId": "vpc-0e69bfbf33bf1046e"
    },
    "status": "CREATING",
    "certificateAuthority": {},
    "platformVersion": "eks.2"
  }
}
C02TH0ZVGTFM:Personal Project i869640$
```

8) Config kubectl

```
~/Documents/ManalisJSU/281/Personal Project — -bash
C02TH0ZVGTFM:~ i869640$ aws sts get-caller-identity
{
  "UserId": "AIDAIYDT56HLLV4XPVGES",
  "Account": "326071200148",
  "Arn": "arn:aws:iam::326071200148:user/AWS_EKSUser_281"
}
C02TH0ZVGTFM:~ i869640$ aws eks update-kubeconfig --name eksCluster
Added new context arn:aws:eks:us-west-2:326071200148:cluster/eksCluster to /Users/i869640/.kube/config
C02TH0ZVGTFM:~ i869640$ kubectl get svc
NAME           TYPE      CLUSTER-IP   EXTERNAL-IP   PORT(S)    AGE
kubernetes     ClusterIP  10.100.0.1  <none>        443/TCP   52m
C02TH0ZVGTFM:~ i869640$
```

9) Configure Worker Node

The screenshot shows the AWS CloudFormation 'Create stack' wizard. The URL in the browser is <https://us-west-2.console.aws.amazon.com/cloudformation/home?region=us-west-2#/stacks/new>. The page title is 'Create stack'. On the left, there's a sidebar with 'Select Template', 'Specify Details', 'Options', and 'Review' buttons. The main area is titled 'Select Template' with the sub-instruction: 'Select the template that describes the stack that you want to create. A stack is a group of related resources that you manage as a single unit.' Below this, there's a 'Design a template' link and a 'Design template' button. Under 'Choose a template', there are three options: 'Select a sample template' (radio button), 'Upload a template to Amazon S3' (radio button), and 'Specify an Amazon S3 template URL' (radio button, which is selected). The URL entered is '-us-west-2.amazonaws.com/cloudformation/2018-11-07/amazon-eks-nodegroup.yaml'. At the bottom right, there are 'Cancel' and 'Next' buttons.



https://us-west-2.console.aws.amazon.com/cloudformation/home?region=us-west-2#/stacks/new

CloudFormation Services - Resource Groups CloudFormation Stacks Create Stack

Create stack

Select Template Specify Details Options Review

Specify Details

Specify a stack name and parameter values. You can use or change the default parameter values, which are defined in the AWS CloudFormation template. Learn more.

Stack name CMPE281-EKS-WorkerNode

Parameters

EKS Cluster

ClusterName eksCluster The cluster name provided when the cluster was created. If it is incorrect, nodes will not be able to join the cluster.

ClusterControlPlane CMPE281-EKS-VPC-ControlPlane SecurityGroup The security group of the cluster control plane.

Worker Node Configuration

NodeGroupName CMPE281-EKS-WorkerNodeGroup Unique identifier for the Node Group.

NodeAutoScalingGroupMinSize 1 Minimum size of Node Group ASG.

NodeAutoScalingGroupMaxSize 3 Maximum size of Node Group ASG.

NodeInstanceType t2.small EC2 instance type for the node instances.

NodeImageId ami-0f54a2f7d2e9c88b3 AMI ID for the node instances.

NodeVolumeSize 20 Node volume size.

KeyName us-west-oregon The EC2 Key Pair to allow SSH access to the instances

BootstrapArguments Arguments to pass to the bootstrap script. See files/bootstrap.sh in https://github.com/awslabs/amazon-eks-ami

Worker Network Configuration

VpcId vpo-0e69bfbf33bf1046e (192... The VPC of the worker instances

Subnets subnet-061a96394001c00cd (192.168.64.0/18) (CMPE281-EKS-V... x subnet-088ec3228fbfc1684 (192.168.192.0/18) (CMPE281-EKS-V... x subnet-09cfadc3366ab9b3 (192.168.128.0/18) (CMPE281-EKS-V... x

The subnets where workers can be created.

10) Configure Guidebook service

```
~/Documents/ManaliJSU/281/Personal Project — bash
~/Documents/ManaliJSU/281/Personal Project — bash

C02TH0ZVGTFM:Personal Project i869640$ kubectl apply -f https://raw.githubusercontent.com/kubernetes/kubernetes/v1.10.3/examples/guestbook-go/redis-master-controller.json
replicationcontroller "redis-master" created
C02TH0ZVGTFM:Personal Project i869640$ kubectl apply -f https://raw.githubusercontent.com/kubernetes/kubernetes/v1.10.3/examples/guestbook-go/redis-master-service.json
service "redis-master" created
C02TH0ZVGTFM:Personal Project i869640$ kubectl apply -f https://raw.githubusercontent.com/kubernetes/kubernetes/v1.10.3/examples/guestbook-go/redis-slave-controller.json
replicationcontroller "redis-slave" created
C02TH0ZVGTFM:Personal Project i869640$ kubectl apply -f https://raw.githubusercontent.com/kubernetes/kubernetes/v1.10.3/examples/guestbook-go/redis-slave-service.json
service "redis-slave" created
C02TH0ZVGTFM:Personal Project i869640$ kubectl apply -f https://raw.githubusercontent.com/kubernetes/kubernetes/v1.10.3/examples/guestbook-go/guestbook-controller.json
replicationcontroller "guestbook" created
C02TH0ZVGTFM:Personal Project i869640$ kubectl apply -f https://raw.githubusercontent.com/kubernetes/kubernetes/v1.10.3/examples/guestbook-go/guestbook-service.json
service "guestbook" created
C02TH0ZVGTFM:Personal Project i869640$ kubectl get services -o wide
NAME          TYPE        CLUSTER-IP   EXTERNAL-IP    PORT(S)        AGE
guestbook     LoadBalancer 10.100.10.248  a0a6ac68df5c311e8bb006e936d175a-175315281.us-west-2.elb.amazonaws.com  3000:30804/TCP  39s
kubernetes   ClusterIP   10.100.0.1    <none>
redis-master  ClusterIP   10.100.220.152  <none>
redis-slave   ClusterIP   10.100.41.29   <none>

C02TH0ZVGTFM:Personal Project i869640$
```

REDIS replication testing

```
~ — kubectl exec -it redis-master-5mhgm -- /bin/bash
C02TH0ZVGTFM:~ i869640$ kubectl get services -o wide
NAME           TYPE      CLUSTER-IP        EXTERNAL-IP
guestbook      LoadBalancer 10.100.10.248   d006ac68df5c311e8bbb006e936d175a-175315281.us-west-2.elb.amazonaws.com
kubernetes     ClusterIP   10.100.0.1       <none>
redis-master   ClusterIP   10.100.220.152  <none>
redis-slave    ClusterIP   10.100.41.29   <none>
C02TH0ZVGTFM:~ i869640$ kubectl get pods
NAME            READY   STATUS    RESTARTS   AGE
guestbook-22g7z 1/1     Running   0          18m
guestbook-9v7mn 1/1     Running   0          18m
guestbook-z6p7r  1/1     Running   0          18m
redis-master-5mhgm 1/1   Running   0          23m
redis-slave-9t2zh 1/1   Running   0          21m
redis-slave-tqgn 1/1   Running   0          21m
C02TH0ZVGTFM:~ i869640$ kubectl exec -it redis-master-5mhgm -- /bin/bash
root@redis-master-5mhgm:/data# redis-cli
127.0.0.1:6379> redis-cli
(error) ERR unknown command 'redis-cli'
127.0.0.1:6379> set FiveGuys 20
OK
127.0.0.1:6379> get FiveGuys
"20"
127.0.0.1:6379>
```

```
~ — kubectl exec -it redis-master-5mhgm -- /bin/bash
Last login: Sat Dec 1 15:57:41 on ttys001
[C02TH0ZVGTFM:~ i869640$ kubectl exec -it redis-slave-9t2zh -- /bin/bash
[ root@redis-slave-9t2zh:/ ]$ redis-cli
127.0.0.1:6379> get FiveGuys
"20"
127.0.0.1:6379>
```