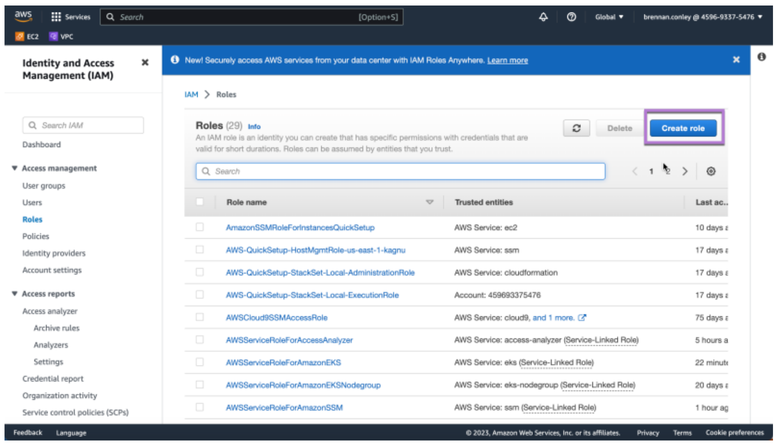
Implementing WEKA on Amazon EKS

Establishing Pre-Requisites

1. Ensure an AWS account with adequate quota is being utilized.
2. Ensure AWS IAM account being used has sufficient roles and policies allocated to create additional IAM roles and policies for the purpose of EKS deployment.
3. Sign into the AWS console and visit https://aws.amazon.com/iam/.
4. Create a new IAM role allowing EC2 resource management and creation by EKS. This role can be referred to as the "Cluster role." The "Cluster role" will later be used as the EKS ***********Cluster service role*********** when creating the EKS cluster.

Click "Create role."

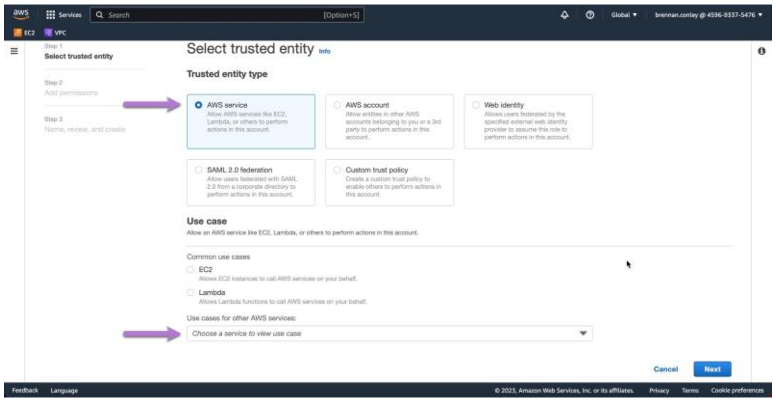


New! Securely access AWS services from your data center with IAM Roles Anywhere. Learn more

Roles (29)
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 ac...
AmazonSSMRoleForInstancesQuickSetup	AWS Service: ec2	10 days a
AWS-QuickSetup-HostMgmtRole-us-east-1-kagnu	AWS Service: ssm	17 days a
AWS-QuickSetup-StackSet-Local-AdministrationRole	AWS Service: cloudformation	17 days a
AWS-QuickSetup-StackSet-Local-ExecutionRole	Account: 459693375476	17 days a
AWSCloud9SSMAccessRole	AWS Service: cloud9, and 1 more.	75 days a
AWSServiceRoleForAccessAnalyzer	AWS Service: access-analyzer (Service-Linked Role)	5 hours a
AWSServiceRoleForAmazonEKS	AWS Service: eks (Service-Linked Role)	22 minut
AWSServiceRoleForAmazonEKSNodegroup	AWS Service: eks-nodegroup (Service-Linked Role)	20 days a
AWSServiceRoleForAmazonSSM	AWS Service: ssm (Service-Linked Role)	1 hour ag

Select the "AWS service" trusted entity type. Then, utilize the indicated drop down.



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.

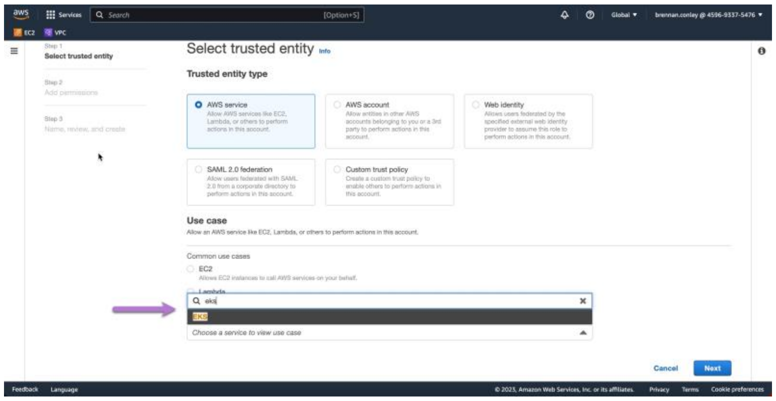
Use case
Allow an AWS service like EC2, Lambda, or others to perform actions in this account.

Common use cases
EC2: Allows EC2 instances to call AWS services on your behalf.
Lambda: Allows Lambda functions to call AWS services on your behalf.

Use cases for other AWS services:
Choose a service to view use case

Cancel Next

Search for and select "EKS." Click "Next."



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.

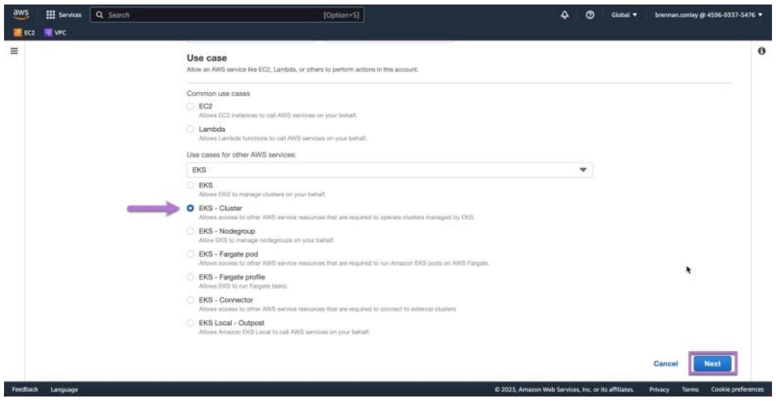
Use case
Allow an AWS service like EC2, Lambda, or others to perform actions in this account.

Common use cases
EC2: Allows EC2 instances to call AWS services on your behalf.
Lambda

eks
EKS
Choose a service to view use case

Cancel Next

From the resulting EKS options, select "EKS - Cluster" and click "Next."



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

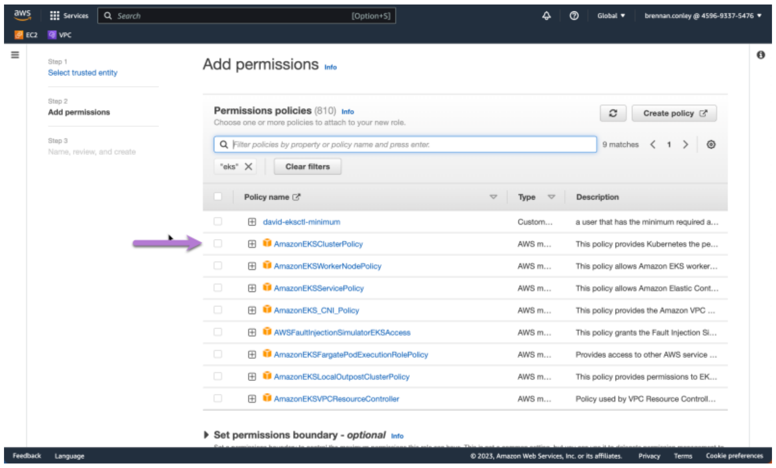
Common use cases
EC2: Allows EC2 instances to call AWS services on your behalf.
Lambda: Allows Lambda functions to call AWS services on your behalf.

Use cases for other AWS services:
EKS

EKS: Allows EKS to manage clusters on your behalf.
[✓ EKS - Cluster] Allows access to other AWS service resources that are required to operate clusters managed by EKS.
EKS - Nodegroup: Allow EKS to manage nodegroups on your behalf.
EKS - Fargate pod: Allows access to other AWS service resources that are required to run Amazon EKS pods on AWS Fargate.
EKS - Fargate profile: Allows EKS to run Fargate tasks.
EKS - Connector: Allows access to other AWS service resources that are required to connect to external clusters
EKS Local - Outpost: Allows Amazon EKS Local to call AWS services on your behalf.

Cancel Next

In the policies search bar, search for “eks.” From the resulting policies, select “AmazonEKSClusterPolicy.”



Permissions policies (810) Info

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

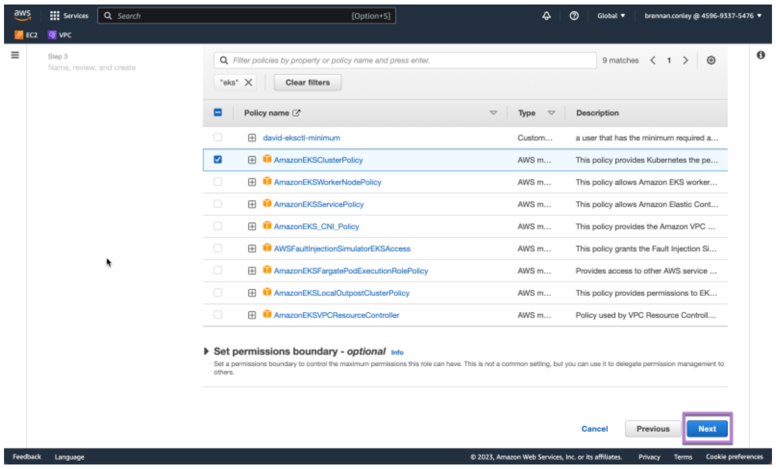
Filter policies by property or policy name and press enter. 9 matches

"eks" Clear filters

Policy name	Type	Description
david-eksctl-minimum	Custom...	a user that has the minimum required a...
AmazonEKSClusterPolicy	AWS m...	This policy provides Kubernetes the pe...
AmazonEKSWorkerNodePolicy	AWS m...	This policy allows Amazon EKS worker...
AmazonEKSServicePolicy	AWS m...	This policy allows Amazon Elastic Cont...
AmazonEKS_CNI_Policy	AWS m...	This policy provides the Amazon VPC ...
AWSFaultInjectionSimulatorEKSAccess	AWS m...	This policy grants the Fault Injection Si...
AmazonEKSFargatePodExecutionRolePolicy	AWS m...	Provides access to other AWS service ...
AmazonEKSLocalOutpostClusterPolicy	AWS m...	This policy provides permissions to EK...
AmazonEKSVPCResourceController	AWS m...	Policy used by VPC Resource Controll...

Set permissions boundary - *optional* Info

Once the policy is selected, click “Next.”



Filter policies by property or policy name and press enter. 9 matches

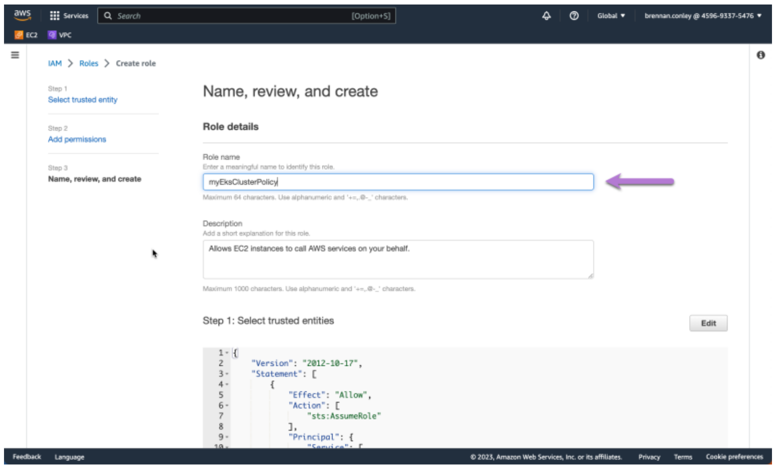
"eks" Clear filters

	Policy name	Type	Description
☐	david-eksctl-minimum	Custom...	a user that has the minimum required a...
✓	AmazonEKSClusterPolicy	AWS m...	This policy provides Kubernetes the pe...
☐	AmazonEKSWorkerNodePolicy	AWS m...	This policy allows Amazon EKS worker...
☐	AmazonEKSServicePolicy	AWS m...	This policy allows Amazon Elastic Cont...
☐	AmazonEKS_CNI_Policy	AWS m...	This policy provides the Amazon VPC ...
☐	AWSFaultInjectionSimulatorEKSAccess	AWS m...	This policy grants the Fault Injection Si...
☐	AmazonEKSFargatePodExecutionRolePolicy	AWS m...	Provides access to other AWS service ...
☐	AmazonEKSLocalOutpostClusterPolicy	AWS m...	This policy provides permissions to EK...
☐	AmazonEKSVPCResourceController	AWS m...	Policy used by VPC Resource Controll...

Set permissions boundary - *optional* Info

Set a permissions boundary to control the maximum permissions this role can have. This is not a common setting, but you can use it to delegate permission management to others.

Provide a name for the role



Name, review, and create

Role details

Role name

Enter a meaningful name to identify this role.

myEksClusterPolicy

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

Description

Add a short explanation for this role.

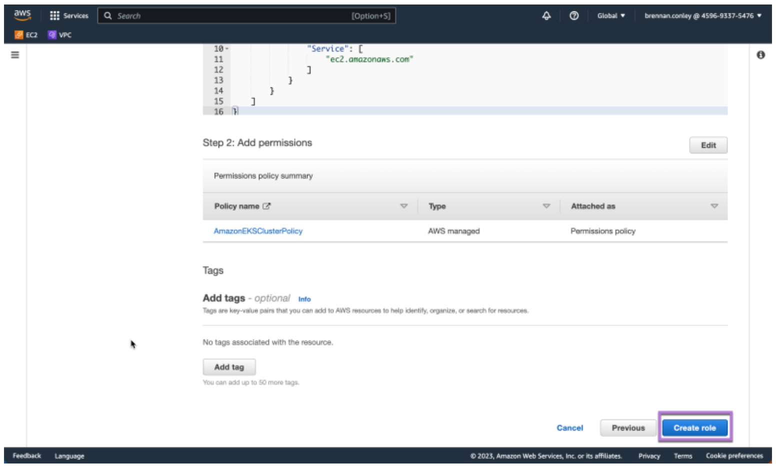
Allows EC2 instances to call AWS services on your behalf.

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

Step 1: Select trusted entities

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "sts:AssumeRole"
            ],
            "Principal": {
```

Click "Create role."



```
            "Service": [
                "ec2.amazonaws.com"
            ]
        }
    }
  ]
}
```

Step 2: Add permissions

Permissions policy summary

Policy name	Type	Attached as
AmazonEKSClusterPolicy	AWS managed	Permissions policy

Tags

Add tags - optional

Tags are key-value pairs that you can add to AWS resources to help identify, organize, or search for resources.

No tags associated with the resource.

You can add up to 50 more tags.

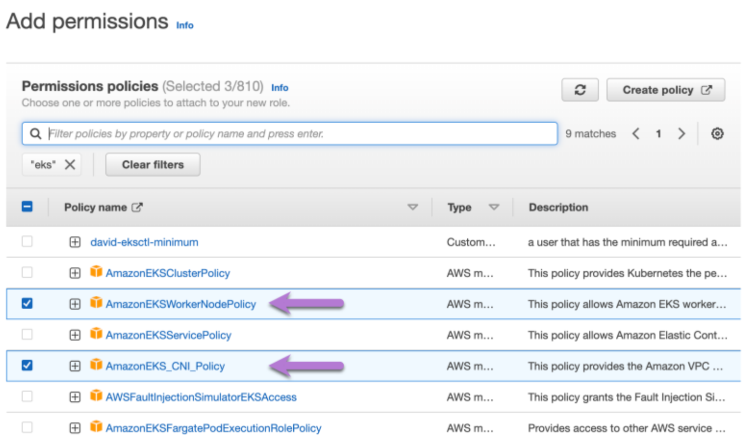
5. Following the same process as above, create another IAM role with *trusted entity type* as "AWS service" and the *use case* as "EC2." This role can be referred to as the "Worker node policy." This time, select the following policies:

   a. "AmazonEKSWorkerNodePolicy"

   b. "AmazonEC2ContainerRegistryReadOnly"

   c. AmazonEKS_CNI_Policy

Create the role. This role will later be used as the EKS node group *Node IAM role*.



Add permissions

Permissions policies (Selected 3/810)

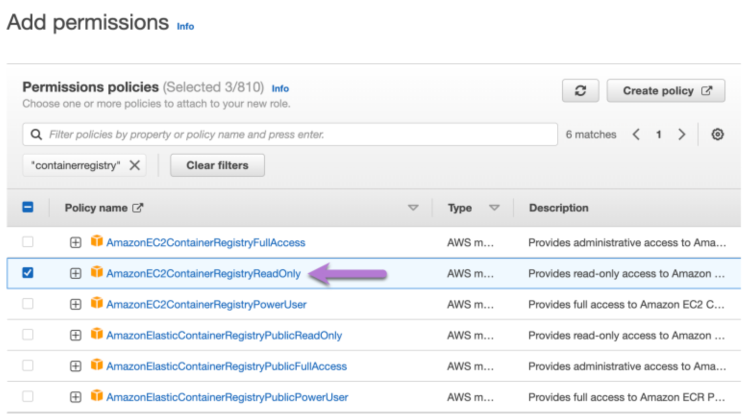
Choose one or more policies to attach to your new role.

9 matches

"eks"

Clear filters

	Policy name	Type	Description
☐	david-eksctl-minimum	Custom…	a user that has the minimum required a…
☐	AmazonEKSClusterPolicy	AWS m…	This policy provides Kubernetes the pe…
✓	AmazonEKSWorkerNodePolicy	AWS m…	This policy allows Amazon EKS worker…
☐	AmazonEKSServicePolicy	AWS m…	This policy allows Amazon Elastic Cont…
✓	AmazonEKS_CNI_Policy	AWS m…	This policy provides the Amazon VPC …
☐	AWSFaultInjectionSimulatorEKSAccess	AWS m…	This policy grants the Fault Injection Si…
☐	AmazonEKSFargatePodExecutionRolePolicy	AWS m…	Provides access to other AWS service …



Add permissions Info

Permissions policies (Selected 3/810) Info

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

Filter policies by property or policy name and press enter. 6 matches

"containerregistry" Clear filters

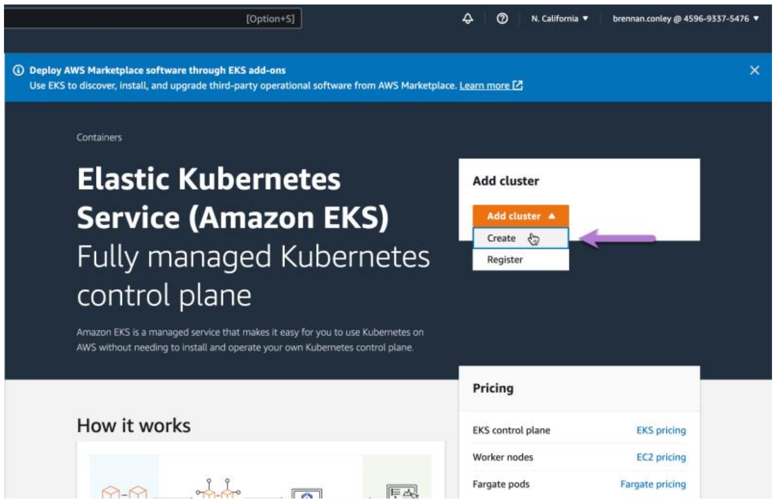
	Policy name	Type	Description
	AmazonEC2ContainerRegistryFullAccess	AWS m...	Provides administrative access to Ama...
✓	AmazonEC2ContainerRegistryReadOnly	AWS m...	Provides read-only access to Amazon ...
	AmazonEC2ContainerRegistryPowerUser	AWS m...	Provides full access to Amazon EC2 C...
	AmazonElasticContainerRegistryPublicReadOnly	AWS m...	Provides read-only access to Amazon ...
	AmazonElasticContainerRegistryPublicFullAccess	AWS m...	Provides administrative access to Ama...
	AmazonElasticContainerRegistryPublicPowerUser	AWS m...	Provides full access to Amazon ECR P...

These two roles will be used later in the EKS deployment process.

6. Ensure that a VPC has been created and is available for use by EKS.
7. Ensure at least two subnets have been created inside the VPC intended for use with EKS. These subnets should have public capabilities i.e. an internet gateway for public network access.
8. Ensure that a security group has been created for use with EKS.
9. Ensure that an AWS public / private key pair has been created, and that the private key has been downloaded and is accessible for use.
10. Either provision a linux jump box in the same VPC containing the Weka cluster and EKS worker nodes, or utilize a laptop configured for SSH communication with machines in the VPC for kubectl commands. Instructions for installing kubectl on various platforms can be found here.
11. In advance, deploy a functional Weka cluster via start.weka.io. Make sure that the management interface is accessible. For the sake of simplicity, deploy the Weka cluster in the same VPC designated for EKS use. If deploying the Weka cluster on a subnet separate from EKS worker nodes, ensure proper subnet routing and security group configuration to allow access between the Weka cluster and EKS worker nodes.

Deploying the EKS cluster

1. To begin, visit aws.amazon.com/eks. Login to the AWS console, and add a cluster.



[Option+S] N. California brennan.conley @ 4596-9337-5476

Deploy AWS Marketplace software through EKS add-ons
Use EKS to discover, install, and upgrade third-party operational software from AWS Marketplace. Learn more

Containers

Elastic Kubernetes Service (Amazon EKS)
Fully managed Kubernetes control plane

Amazon EKS is a managed service that makes it easy for you to use Kubernetes on AWS without needing to install and operate your own Kubernetes control plane.

Add cluster
Add cluster
Create
Register

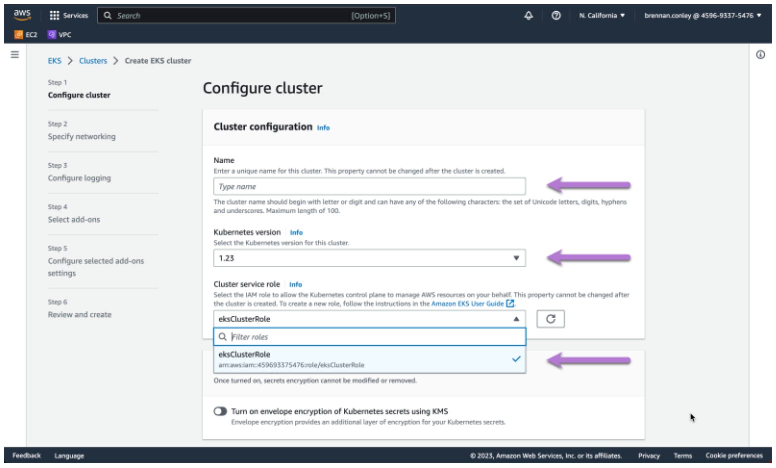
Pricing

EKS control plane	EKS pricing
Worker nodes	EC2 pricing
Fargate pods	Fargate pricing

How it works

2. Configure the cluster.

Enter an EKS cluster name. Select Kubernetes version 1.23. The default version of 1.24 currently (at the time of writing) has a bug that does not allow kubectl to properly communicate with the EKS cluster management interface. The actual issue is with kubectl, Kubernetes itself. For reference, the version of kubectl used must be -1, equal to, or +1 the version of the Kubernetes cluster. For *Cluster service role* select the "Cluster role" IAM role created in step 4 of the prerequisites section.



Services Search [Option+S] N. California brennan.conley @ 4596-9337-5476
EC2 VPC

EKS > Clusters > Create EKS cluster

Step 1 Configure cluster
Step 2 Specify networking
Step 3 Configure logging
Step 4 Select add-ons
Step 5 Configure selected add-ons settings
Step 6 Review and create

Configure cluster

Cluster configuration Info

Name
Enter a unique name for this cluster. This property cannot be changed after the cluster is created.
Type name
The cluster name should begin with letter or digit and can have any of the following characters: the set of Unicode letters, digits, hyphens and underscores. Maximum length of 100.

Kubernetes version Info
Select the Kubernetes version for this cluster.
1.23

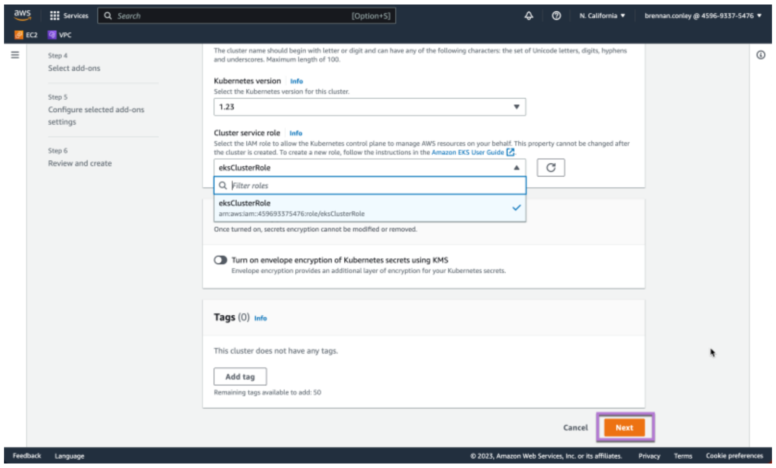
Cluster service role Info
Select the IAM role to allow the Kubernetes control plane to manage AWS resources on your behalf. This property cannot be changed after the cluster is created. To create a new role, follow the instructions in the Amazon EKS User Guide.
eksClusterRole
Filter roles
eksClusterRole
arn:aws:iam::459693375476:role/eksClusterRole

Once turned on, secrets encryption cannot be modified or removed.

Turn on envelope encryption of Kubernetes secrets using KMS
Envelope encryption provides an additional layer of encryption for your Kubernetes secrets.

Feedback Language © 2023, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Leave all other options as default and click "Next."



The cluster name should begin with letter or digit and can have any of the following characters: the set of Unicode letters, digits, hyphens and underscores. Maximum length of 100.

Kubernetes version
Select the Kubernetes version for this cluster.
1.23

Cluster service role
Select the IAM role to allow the Kubernetes control plane to manage AWS resources on your behalf. This property cannot be changed after the cluster is created. To create a new role, follow the instructions in the Amazon EKS User Guide.
eksClusterRole

eksClusterRole ✓
arn:aws:iam::459693375476:role/eksClusterRole

Once turned on, secrets encryption cannot be modified or removed.

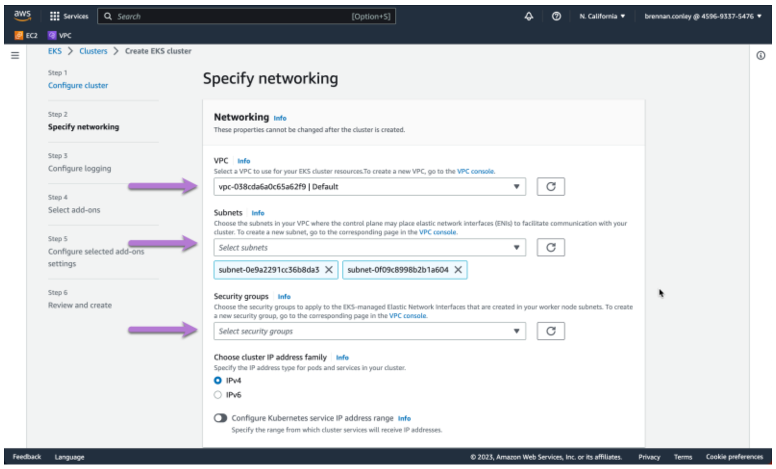
Turn on envelope encryption of Kubernetes secrets using KMS
Envelope encryption provides an additional layer of encryption for your Kubernetes secrets.

Tags (0)

This cluster does not have any tags.

Remaining tags available to add: 50

Continue cluster configuration by selecting the VPC, subnets, and security group created in the prerequisites section. EKS requires at least two subnets to be selected for load-balancing and redundancy purposes. Use the default of IPv4. Leave the Kubernetes service IP address range as default.



Specify networking

Networking
These properties cannot be changed after the cluster is created.

VPC
Select a VPC to use for your EKS cluster resources.To create a new VPC, go to the VPC console.
vpc-038cda6a0c65a62f9 | Default

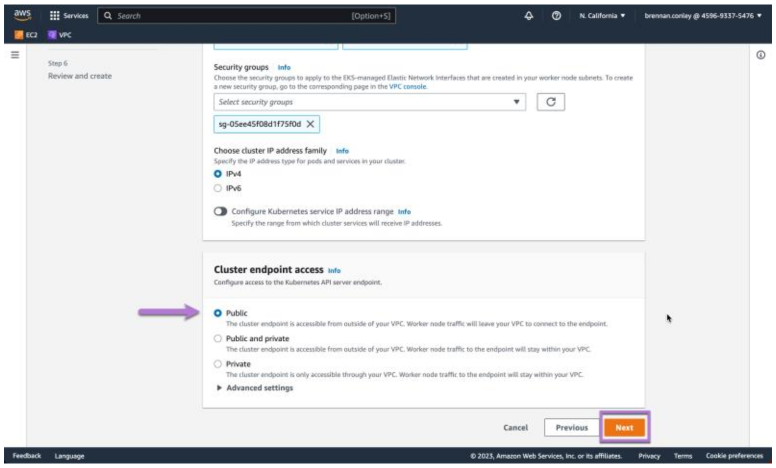
Subnets
Choose the subnets in your VPC where the control plane may place elastic network interfaces (ENIs) to facilitate communication with your cluster. To create a new subnet, go to the corresponding page in the VPC console.
Select subnets
subnet-0e9a2291cc36b8da3
subnet-0f09c8998b2b1a604

Security groups
Choose the security groups to apply to the EKS-managed Elastic Network Interfaces that are created in your worker node subnets. To create a new security group, go to the corresponding page in the VPC console.
Select security groups

Choose cluster IP address family
Specify the IP address type for pods and services in your cluster.
[✓ IPv4] IPv6

Configure Kubernetes service IP address range
Specify the range from which cluster services will receive IP addresses.

Under *Cluster endpoint access*, select the default of "Public." Click "Next."



Step 6
Review and create

Security groups Info
Choose the security groups to apply to the EKS-managed Elastic Network Interfaces that are created in your worker node subnets. To create a new security group, go to the corresponding page in the VPC console.
Select security groups
sg-05ee45f08d1f75f0d

Choose cluster IP address family Info
Specify the IP address type for pods and services in your cluster.
[✓ IPv4]
IPv6

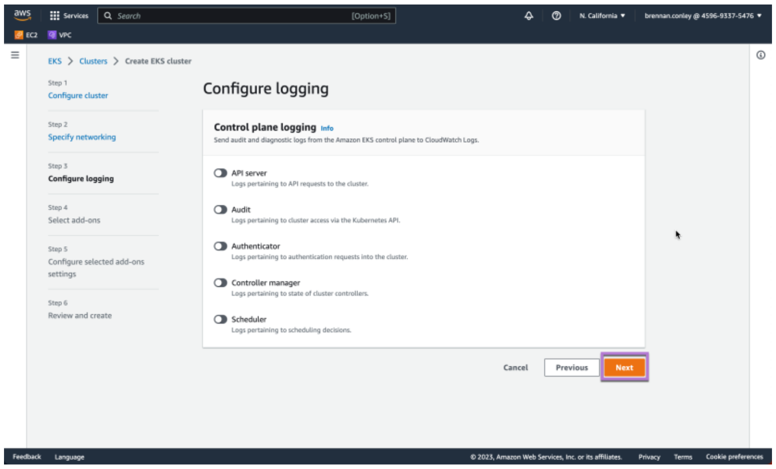
Configure Kubernetes service IP address range Info
Specify the range from which cluster services will receive IP addresses.

Cluster endpoint access Info
Configure access to the Kubernetes API server endpoint.

[✓ Public]
The cluster endpoint is accessible from outside of your VPC. Worker node traffic will leave your VPC to connect to the endpoint.
Public and private
The cluster endpoint is accessible from outside of your VPC. Worker node traffic to the endpoint will stay within your VPC.
Private
The cluster endpoint is only accessible through your VPC. Worker node traffic to the endpoint will stay within your VPC.
Advanced settings

Cancel Previous Next

Configure logging as necessary, then click "Next."



EKS > Clusters > Create EKS cluster

Step 1
Configure cluster
Step 2
Specify networking
Step 3
Configure logging
Step 4
Select add-ons
Step 5
Configure selected add-ons settings
Step 6
Review and create

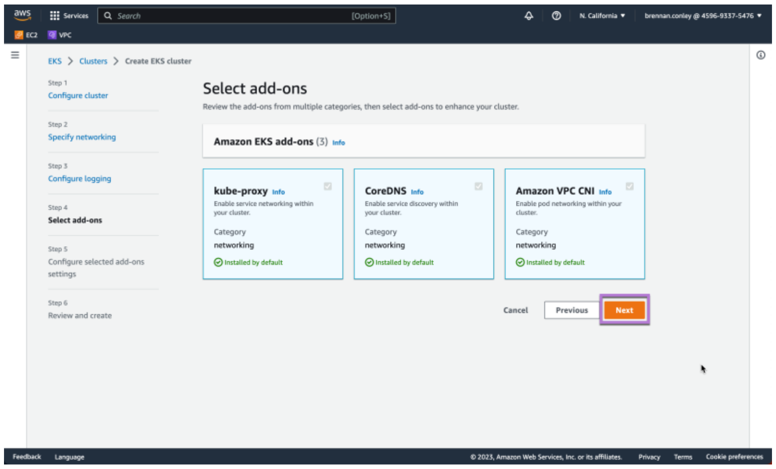
Configure logging

Control plane logging Info
Send audit and diagnostic logs from the Amazon EKS control plane to CloudWatch Logs.

API server
Logs pertaining to API requests to the cluster.
Audit
Logs pertaining to cluster access via the Kubernetes API.
Authenticator
Logs pertaining to authentication requests into the cluster.
Controller manager
Logs pertaining to state of cluster controllers.
Scheduler
Logs pertaining to scheduling decisions.

Cancel Previous Next

Under *Select add-ons* note the defaults and click "Next."



EKS > Clusters > Create EKS cluster

Step 1
Configure cluster
Step 2
Specify networking
Step 3
Configure logging
Step 4
Select add-ons
Step 5
Configure selected add-ons settings
Step 6
Review and create

Select add-ons
Review the add-ons from multiple categories, then select add-ons to enhance your cluster.

Amazon EKS add-ons (3) Info

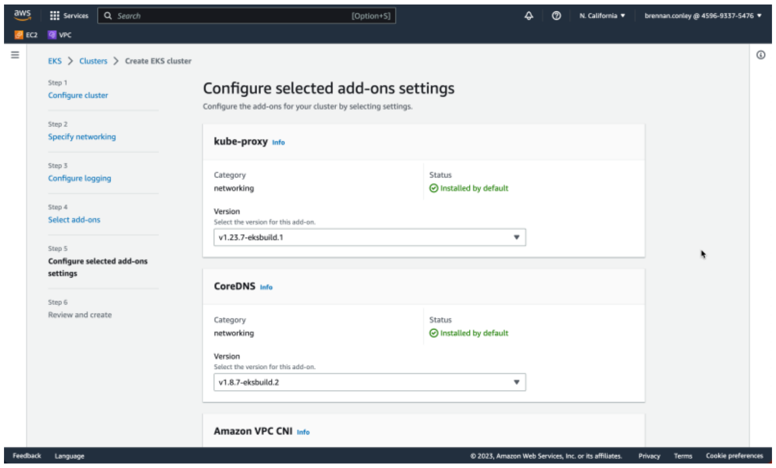
kube-proxy Info
Enable service networking within your cluster.
Category
networking
Installed by default

CoreDNS Info
Enable service discovery within your cluster.
Category
networking
Installed by default

Amazon VPC CNI Info
Enable pod networking within your cluster.
Category
networking
Installed by default

Cancel Previous Next

Under *Configure selected add-ons settings* note the defaults and click "Next."



Configure selected add-ons settings

Configure the add-ons for your cluster by selecting settings.

kube-proxy Info

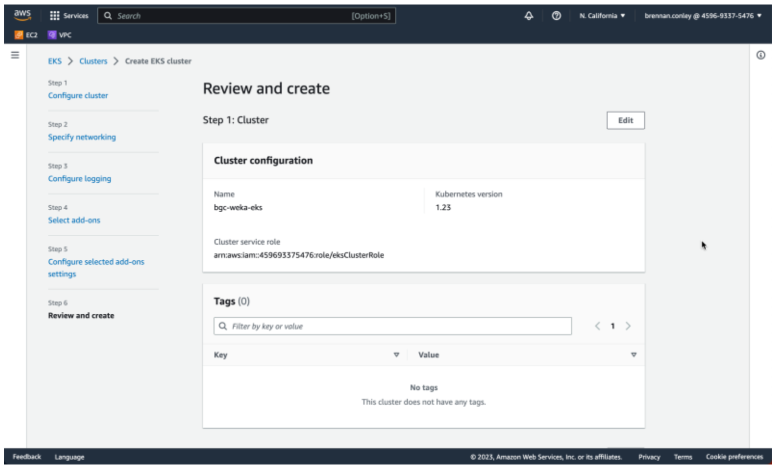
Category: networking
Status: Installed by default
Version: Select the version for this add-on. v1.23.7-eksbuild.1

CoreDNS Info

Category: networking
Status: Installed by default
Version: Select the version for this add-on. v1.8.7-eksbuild.2

Amazon VPC CNI Info

Finally, under *Review and create* review all configured options and click "Create." The EKS cluster management framework will be created and necessary services started. No EKS worker nodes or node groups will be created at this time. Cluster creation will take approximately 10 minutes.



Review and create

Step 1: Cluster

Cluster configuration

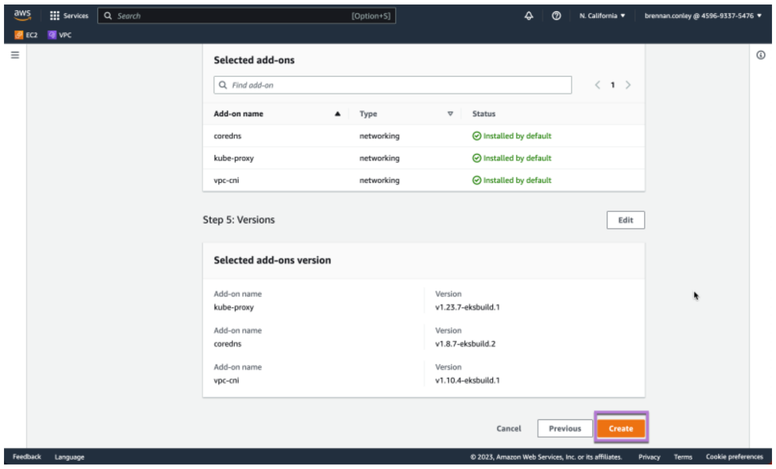
Name: bgc-weka-eks
Kubernetes version: 1.23
Cluster service role: arn:aws:iam::459693375476:role/eksClusterRole

Tags (0)

Filter by key or value

Key	Value

No tags
This cluster does not have any tags.



Selected add-ons

Find add-on

Add-on name	Type	Status
coredns	networking	Installed by default
kube-proxy	networking	Installed by default
vpc-cni	networking	Installed by default

Step 5: Versions

Selected add-ons version

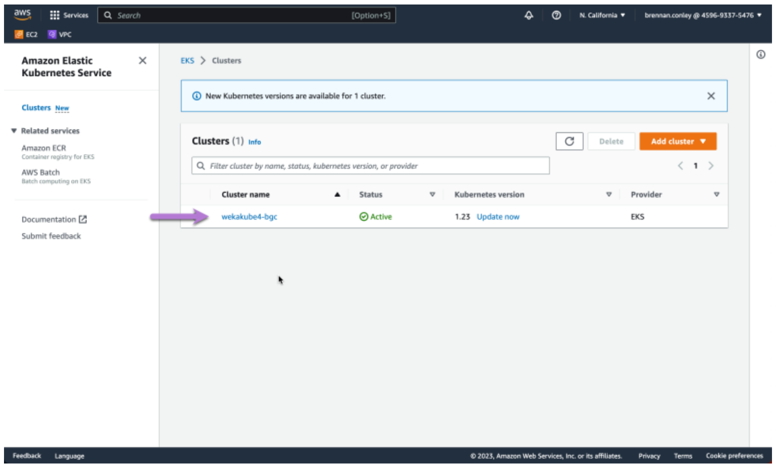
Add-on name	Version
kube-proxy	v1.23.7-eksbuild.1
coredns	v1.8.7-eksbuild.2
vpc-cni	v1.10.4-eksbuild.1

Creating node groups - non-autoscaling

After the cluster has been created, a node group must be provisioned in order to deploy pods. Pods will contain worker nodes allocated from a worker node group. The following instructions will outline how to create a worker node group.

1. Navigate to EKS compute resources

Under *EKS*, *Clusters*, locate and select the previously created cluster.



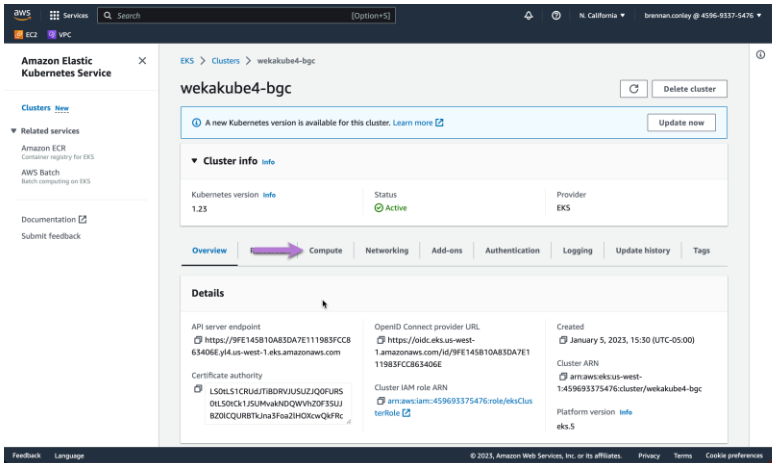
New Kubernetes versions are available for 1 cluster.

Clusters (1) Info

Filter cluster by name, status, kubernetes version, or provider

Cluster name	Status	Kubernetes version	Provider
wekakube4-bgc	Active	1.23 Update now	EKS

Select "Compute."



wekakube4-bgc

A new Kubernetes version is available for this cluster. Learn more

Cluster info Info

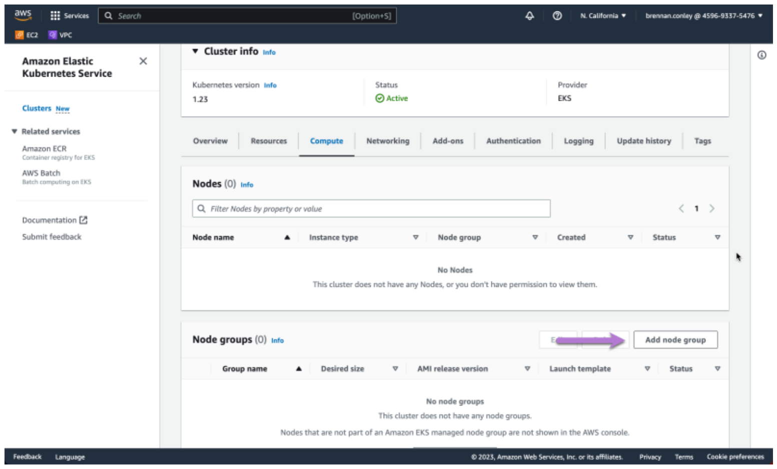
Kubernetes version Info: 1.23
Status: Active
Provider: EKS

Details

API server endpoint: https://9FE145B10A83DA7E111983FCC863406E.yl4.us-west-1.eks.amazonaws.com
Certificate authority: LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCk1JSUMvakNDQWVhZ0F3SUJBZ0lCQURBTkJna3Foa2lHOXcwQkFRc
OpenID Connect provider URL: https://oidc.eks.us-west-1.amazonaws.com/id/9FE145B10A83DA7E111983FCC863406E
Cluster IAM role ARN: arn:aws:iam::459693375476:role/eksClusterRole
Created: January 5, 2023, 15:30 (UTC-05:00)
Cluster ARN: arn:aws:eks:us-west-1:459693375476:cluster/wekakube4-bgc
Platform version Info: eks.5

2. Create the node group

Scroll down and select "Add node group."



Cluster info Info

Kubernetes version Info	Status	Provider
1.23	Active	EKS

Nodes (0) Info

Filter Nodes by property or value

Node name	Instance type	Node group	Created	Status

No Nodes

This cluster does not have any Nodes, or you don't have permission to view them.

Node groups (0) Info

Group name	Desired size	AMI release version	Launch template	Status

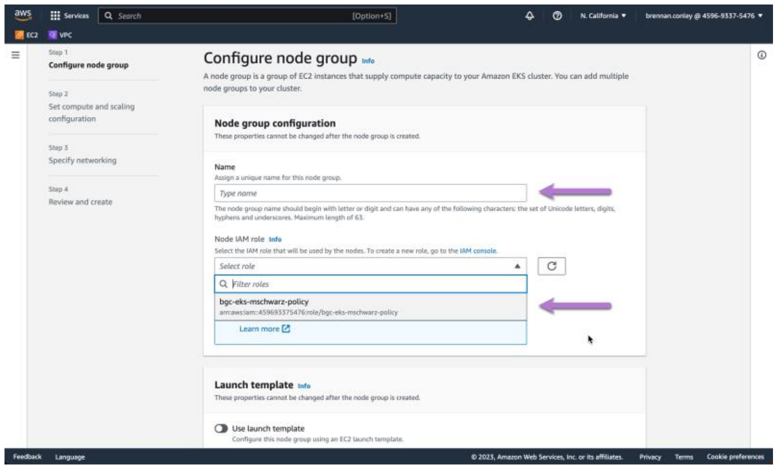
No node groups

This cluster does not have any node groups.

Nodes that are not part of an Amazon EKS managed node group are not shown in the AWS console.

© 2023, Amazon Web Services, Inc. or its affiliates.

Under *Configure the node group* provide a name for the node group. For *Node IAM role* select the second IAM role created in the prerequisites section as the "Worker node policy." Leave all other options as default. Click "Next."



Configure node group Info

A node group is a group of EC2 instances that supply compute capacity to your Amazon EKS cluster. You can add multiple node groups to your cluster.

Node group configuration

These properties cannot be changed after the node group is created.

Name

Assign a unique name for this node group.

Type name

The node group name should begin with letter or digit and can have any of the following characters: the set of Unicode letters, digits, hyphens and underscores. Maximum length of 63.

Node IAM role Info

Select the IAM role that will be used by the nodes. To create a new role, go to the IAM console.

Select role

Filter roles

bgc-eks-mschwarz-policy
arn:aws:iam::459693375476:role/bgc-eks-mschwarz-policy

Learn more

Launch template Info

These properties cannot be changed after the node group is created.

Use launch template

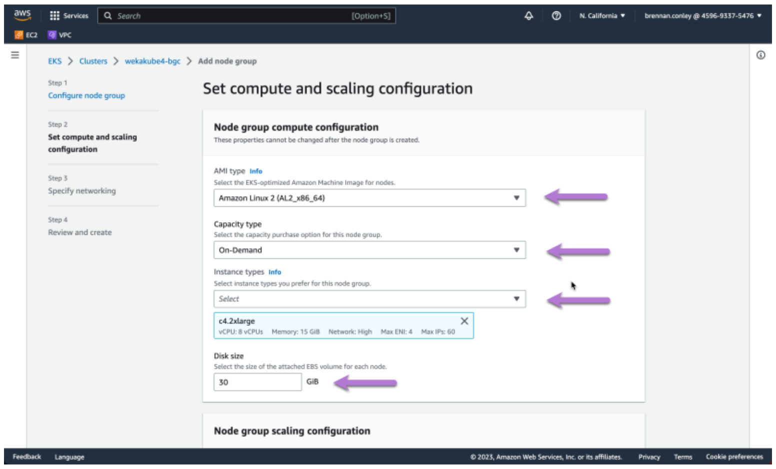
Configure this node group using an EC2 launch template.

© 2023, Amazon Web Services, Inc. or its affiliates.

Under *Set compute and scaling information* configure desired compute and scaling parameters for the node group worker nodes.

For the purposes of this guide, select ***Amazon Linux 2 (AL2_x86_64)*** for the *AMI type*. For *capacity type* select *On-Demand*.

Select the *c4.2xlarge (or otherwise desired instance size)* under *Instance types*. Allocate *30GiB* for the *Disk size*.



Set compute and scaling configuration

Node group compute configuration

These properties cannot be changed after the node group is created.

AMI type Info

Select the EKS-optimized Amazon Machine Image for nodes.

Amazon Linux 2 (AL2_x86_64)

Capacity type

Select the capacity purchase option for this node group.

On-Demand

Instance types Info

Select instance types you prefer for this node group.

Select

c4.2xlarge

vCPU: 8 vCPUs Memory: 15 GiB Network: High Max ENI: 4 Max IPs: 60

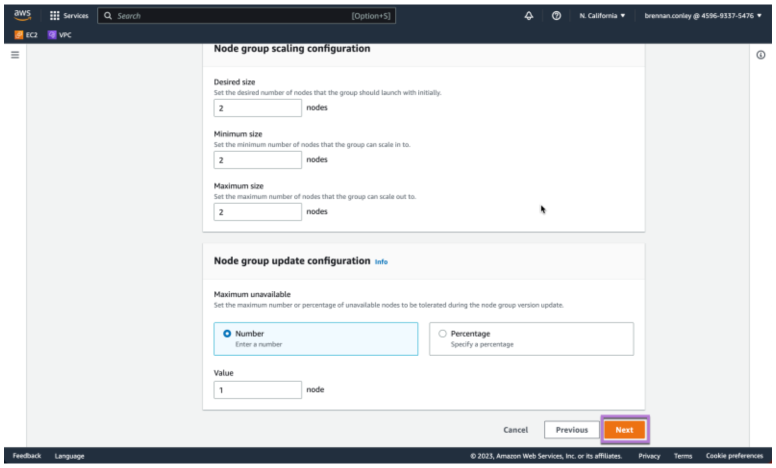
Disk size

Select the size of the attached EBS volume for each node.

30 GiB

Node group scaling configuration

Select desired values for *Node group scaling configuration* and *Node group update configuration*. It's fine to leave the default values, unless a specific cluster size or scaling configuration is desired. Click "Next."



Node group scaling configuration

Desired size

Set the desired number of nodes that the group should launch with initially.

2 nodes

Minimum size

Set the minimum number of nodes that the group can scale in to.

2 nodes

Maximum size

Set the maximum number of nodes that the group can scale out to.

2 nodes

Node group update configuration Info

Maximum unavailable

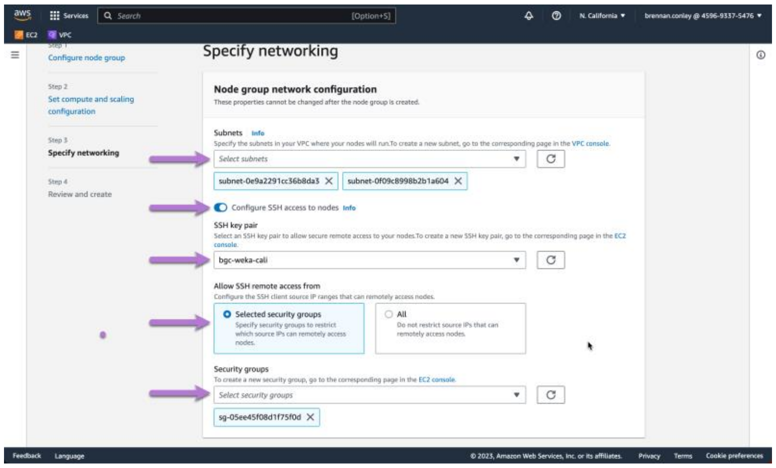
Set the maximum number or percentage of unavailable nodes to be tolerated during the node group version update.

[✓ Number] Enter a number — Percentage Specify a percentage

Value

1 node

Specify networking. Under *Node group network configuration* select the subnets previously created for EKS in the prerequisites section. Toggle *Configure SSH access to nodes* to "on." Click "Next."



Specify networking

Node group network configuration

These properties cannot be changed after the node group is created.

Subnets Info

Specify the subnets in your VPC where your nodes will run.To create a new subnet, go to the corresponding page in the VPC console.

Select subnets

subnet-0e9a2291cc36b8da3 ✕ subnet-0f09c8998b2b1a604 ✕

Configure SSH access to nodes Info

SSH key pair

Select an SSH key pair to allow secure remote access to your nodes.To create a new SSH key pair, go to the corresponding page in the EC2 console.

bgc-weka-cali

Allow SSH remote access from

Configure the SSH client source IP ranges that can remotely access nodes.

[✓ Selected security groups] Specify security groups to restrict which source IPs can remotely access nodes.

All — Do not restrict source IPs that can remotely access nodes.

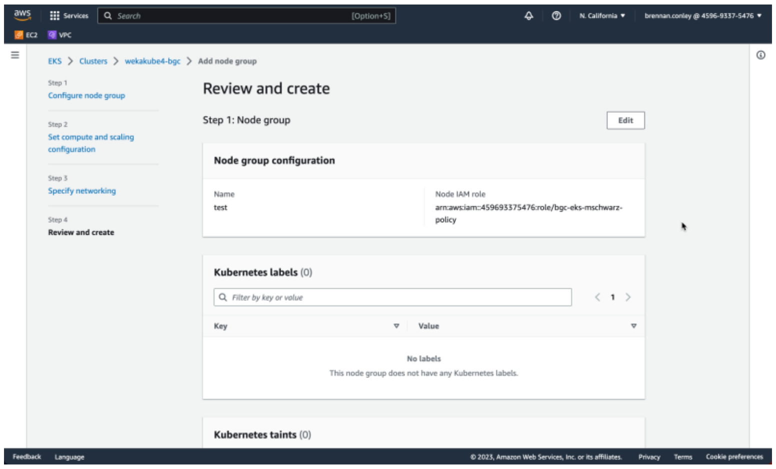
Security groups

To create a new security group, go to the corresponding page in the EC2 console.

Select security groups

sg-05ee45f08d1f75f0d ✕

Review the configuration and parameter selection. If everything looks acceptable, click "Create."



Review and create

Step 1: Node group

Node group configuration

Name	Node IAM role
test	arn:aws:iam::459693375476:role/bgc-eks-mschwarz-policy

Kubernetes labels (0)

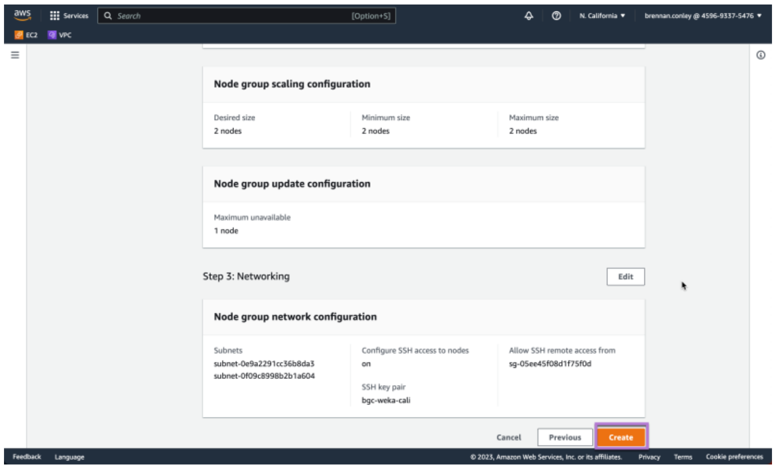
Filter by key or value

Key	Value

No labels

This node group does not have any Kubernetes labels.

Kubernetes taints (0)



Node group scaling configuration

Desired size	Minimum size	Maximum size
2 nodes	2 nodes	2 nodes

Node group update configuration

Maximum unavailable

1 node

Step 3: Networking

Node group network configuration

Subnets	Configure SSH access to nodes	Allow SSH remote access from
subnet-0e9a2291cc36b8da3 subnet-0f09c8998b2b1a604	on SSH key pair bgc-weka-cali	sg-05ee45f08d1f75f0d

Configuring autoscaling deployments and node groups

Pre-requisites

This section assumes the following:

- A Weka cluster has been deployed using start.weka.io and has the requisite amount of storage to support the workload being deployed via Kubernetes.
- The default Weka admin password has been changed and login credentials are available to be used by the CSI secrets YAML file.
- A small-scale file system (named something similar to "eksclient") has been created on the Weka cluster and will not be used for storing application data. This file system can be thin provisioned. A volume with minimum capacity of 5GB and a maximum capacity of 10GB is sufficient.
- YAML example files can be found on docs.weka.io in the CSI plugin section. These example files assume a filesystem named "default" and a nested directory named "shared" with the proper permissions for EKS worker node access. Executing chmod 777 on the "shared" directory from a system with access to the Weka storage will provide the quickest route to granting access.
- An EKS cluster and node group have been created using the instructions earlier in this documentation.

Supporting resources

Client installation script

This script should be saved in an S3 bucket which is accessible to the EKS worker node EC2 instances or any other EC2 instances which require Weka client installation.

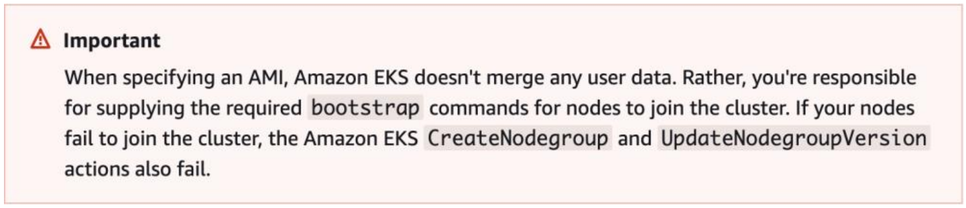
Code snippet for launch template user data

This code will be used in the launch template user data.

Obtaining Kubernetes User Data and Creating the Launch Template

Autoscaling groups in Amazon EKS allow for dynamic provisioning (or removal) of EKS worker nodes based upon user specified criteria or defined environmental parameters (CPU utilization, memory utilization, etc). The node groups can also be scaled manually by altering the number of nodes allocated in the related node group settings. In this example, the latter method will be used to increase / decrease node count within the node group.

Amazon AWS Launch Templates allow for various commands or scripts to be run upon instantiation of an EC2 instance. Launch Templates can be thought of as similar - but not identical - to first boot scripts. In the context of Kubernetes, launch templates are used to bootstrap Kubernetes. It is important to note that manually adding to the Launch Template of an existing worker nodes will not merge the new user data with the Kubernetes bootstrap scripts.



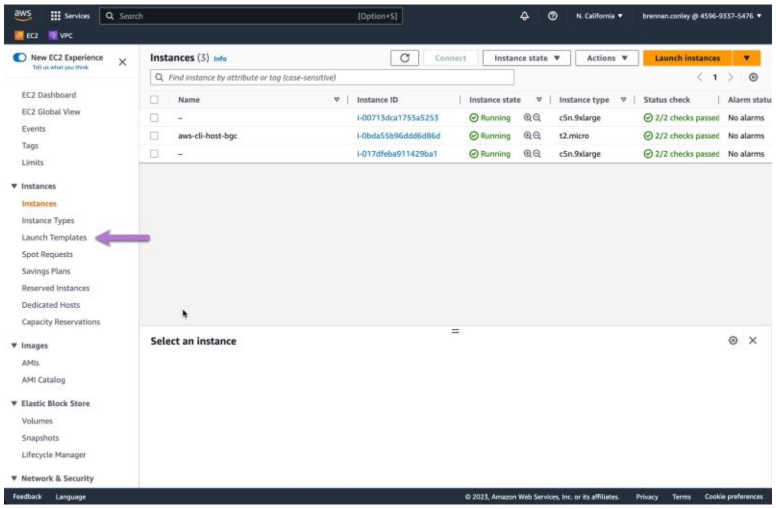
Important

When specifying an AMI, Amazon EKS doesn't merge any user data. Rather, you're responsible for supplying the required `bootstrap` commands for nodes to join the cluster. If your nodes fail to join the cluster, the Amazon EKS `CreateNodegroup` and `UpdateNodegroupVersion` actions also fail.

Due to this important nuance, we will need to examine the user data from an existing or temporarily created EKS node group. The instructions provided earlier in this documentation can be used to create the temporary node group, if necessary.

1. Obtain user data for the existing or newly created EKS worker nodes.

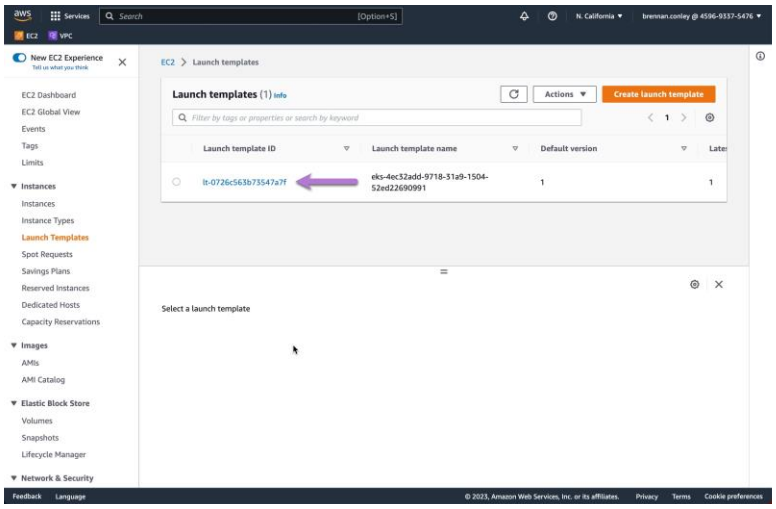
In the AWS console, navigate to the EC2 pane. Select "*Launch Templates*" from the left hand navigation pane.



Instances (3) Info

Name	Instance ID	Instance state	Instance type	Status check	Alarm statu
–	i-00713dca1755a5253	Running	c5n.9xlarge	2/2 checks passed	No alarms
aws-cli-host-bgc	i-0bda55b96ddd6d86d	Running	t2.micro	2/2 checks passed	No alarms
–	i-017dfeba911429ba1	Running	c5n.9xlarge	2/2 checks passed	No alarms

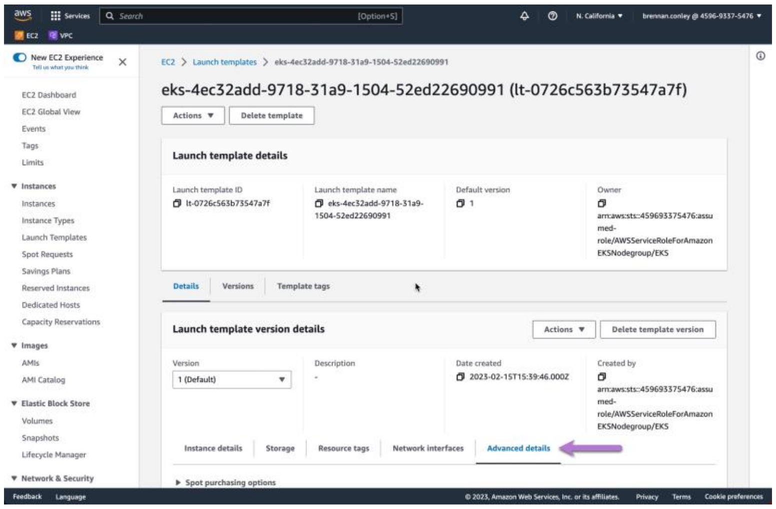
On the *Launch Templates* page, select the Launch Template associated with the existing or newly created EKS node group.



Launch templates (1) Info

Launch template ID	Launch template name	Default version	Late
lt-0726c563b73547a7f	eks-4ec32add-9718-31a9-1504-52ed22690991	1	1

Once on the EKS *Launch Template* page, select "*Advanced details*."



EC2 > Launch templates > eks-4ec32add-9718-31a9-1504-52ed22690991

eks-4ec32add-9718-31a9-1504-52ed22690991 (lt-0726c563b73547a7f)

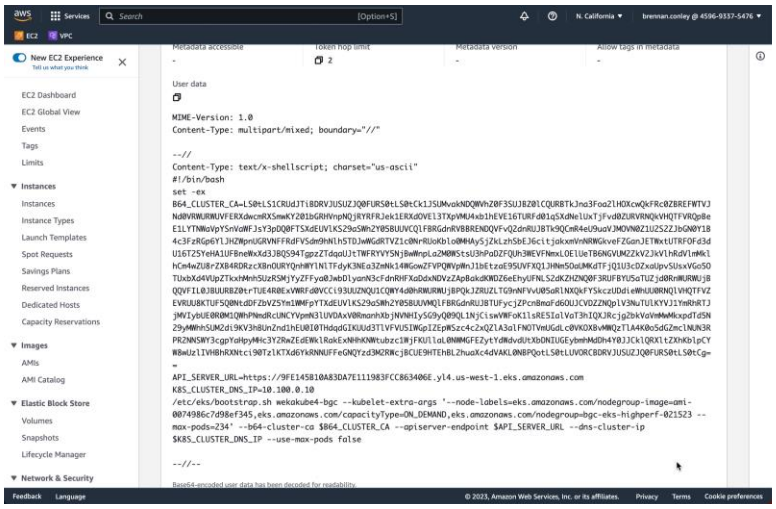
Launch template details

Launch template ID	Launch template name	Default version	Owner
lt-0726c563b73547a7f	eks-4ec32add-9718-31a9-1504-52ed22690991	1	arn:aws:sts::459693375476:assumed-role/AWSServiceRoleForAmazonEKSNodegroup/EKS

Launch template version details

Version	Description	Date created	Created by
1 (Default)	-	2023-02-15T15:39:46.000Z	arn:aws:sts::459693375476:assumed-role/AWSServiceRoleForAmazonEKSNodegroup/EKS

Under the *Advanced details* page, scroll down to view the applicable user data script which is used to bootstrap the EKS worker node EC2 instances into the EKS cluster. Please note, this user data is specific to your EKS cluster. This script will be used later when creating the Launch Template.



Metadata accessible	Token hop limit	Metadata version	Allow tags in metadata
-	2	-	-

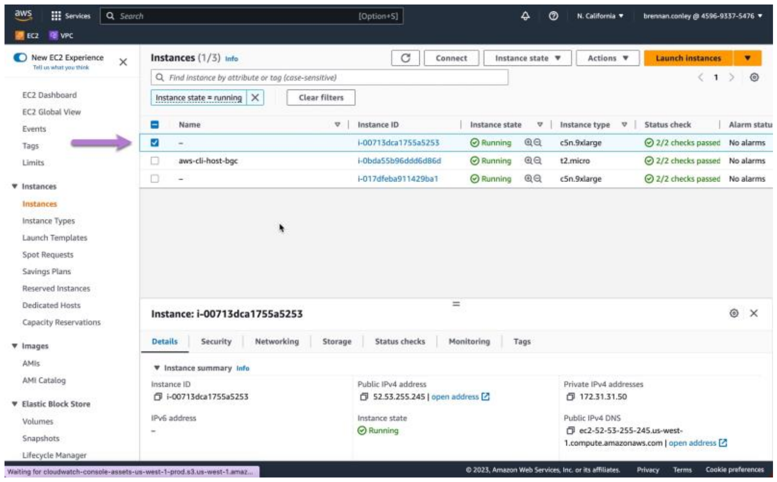
User data

```
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="//"

--//
Content-Type: text/x-shellscript; charset="us-ascii"
#!/bin/bash
set -ex
B64_CLUSTER_CA=LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCk1JSUMvakNDQWVhZ0F3SUJBZ0lCQURBTkJna3Foa2lHOXcwQkFRc0ZBREFWTVJ
Nd0VRWURWUVFERXdwcmRXSmwKY201bGRHVnpNQjRYRFRJek1ERXdOVEl3TXpVMU4xb1hEVE16TURFd01qSXdNelUxTjFvd0ZURVRNQkVHQTFVRQpBe
E1LYTNWaVpYSnVaWFJsY3pDQ0FTSXdEUVlKS29aSWh2Y05BUUVCQlFBRGdnRVBBRENDQVFvQ2dnRUJBTk9QCmR4eU9uaVJMOVN0Z1U2S2ZJbGN0Y1B
4c3FzRGp6YlJHZWpnUGRVNFFRdFVSdm9hNlh5TDJwWGdRTVZ1c0NrRUoKblo0MHAySjZkLzhSbEJ6citjakxmVnNRWGkveFZGanJETWxtUTRFOFd3d
U16T25YeHA1UFBneWxXd3JBQS94TgpzZTdqaUJtTWFRYVYSNjBwWnpLa2M0WStsU3hPaDZFQUh3WEVFNmxLOElUeTB6NGVUM2ZkV2JkVlhRdVlmMkl
hCm4wZU8rZXB4RDRzcXBnOURYQnhWYlNlTFdyK3NEa3ZmNk14WGowZFVPQWVpWnJ1bEtzaE95UVFXQ1JHNm5OaUMKdTFjQ1U3cDZxaUpvSUsxVGo5O
TUxbXd4VUpZTkxhMnh5UzRSMjYyZFFya0JwbDlyanN3cFdnRHFXaDdxNDVzZApBakdKWDZ6eEhyUFNLS2dKZHZNQ0F3RUFBYU5aTUZjd0RnWURWUjB
QQVFIL0JBUURBZ0trTUE4R0ExVWRFd0VCCi93UUZNQU1CQWY4d0hRWURWUjBPQkJZRUZLTG9nNFVvU05aRlNXQkFYSkczUDdieWhUU0RNQlVHQTFVZ
EVRUU8KTUF5Q0NtdDFZbVZ5Ym1WMFpYTXdEUVlKS29aSWh2Y05BUUVMQlFBRGdnRUJBTUFycjZPcnBmaFd6OUJCVDZZNQplV3NuTUlKYVJ1YmRhRTJ
jMVIybUE0R0M1QWhPNmdRcUNCYVpmN3lUVDAxV0RmanhXbjNVNHIySG9yQ09QL1NjCiswVWFoK1lsRE5IalVaT3hIQXJRcjg2bkVaVmMwMkxpdTd5N
29yMWhhSUM2di9KV3h8UnZnd1hEU0I0THdqdGIKUUd3TlVFVU5IWGpIZEpWSzc4c2xQZlA3alFNOTVmUGdLc0VKOXBvMWQzTlA4K0o5dGZmclNUN3R
PRZNNSWY3cgpYaHpyMHc3Y2RwZEdEWklRakExNHhKNWtubzc1WjFKUllaL0NWMGFEZytYdWdvdUtXbDNIUGEybmhMdDh4Y0JJCklQRXltZXhKblpCY
W8wUzlIVHBhRXNtci90TzlKTXd6YkRNNUFFeGNQYzd3M2RWcjBCUE9HTEhBL2huaXc4dVAKL0NBPQotLS0tLUVORCBDRVJUSUZJQ0FURS0tLS0tCg=
=
API_SERVER_URL=https://9FE145B10A83DA7E111983FCC863406E.yl4.us-west-1.eks.amazonaws.com
K8S_CLUSTER_DNS_IP=10.100.0.10
/etc/eks/bootstrap.sh wekakube4-bgc --kubelet-extra-args '--node-labels=eks.amazonaws.com/nodegroup-image=ami-
0074986c7d98ef345,eks.amazonaws.com/capacityType=ON_DEMAND,eks.amazonaws.com/nodegroup=bgc-eks-highperf-021523 --
max-pods=234' --b64-cluster-ca $B64_CLUSTER_CA --apiserver-endpoint $API_SERVER_URL --dns-cluster-ip
$K8S_CLUSTER_DNS_IP --use-max-pods false

--//--
```

Base64-encoded user data has been decoded for readability.

2. Create the new Launch Template.

Navigate to the EC2 instances page and select one of the EKS worker node EC2 instances.

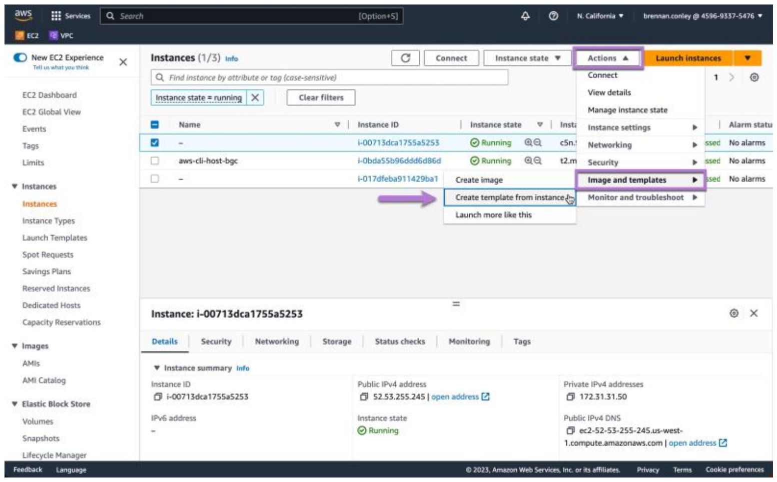


	Name	Instance ID	Instance state	Instance type	Status check	Alarm statu
✓	–	i-00713dca1755a5253	Running	c5n.9xlarge	2/2 checks passed	No alarms
	aws-cli-host-bgc	i-0bda55b96ddd6d86d	Running	t2.micro	2/2 checks passed	No alarms
	–	i-017dfeba911429ba1	Running	c5n.9xlarge	2/2 checks passed	No alarms

Instance: i-00713dca1755a5253

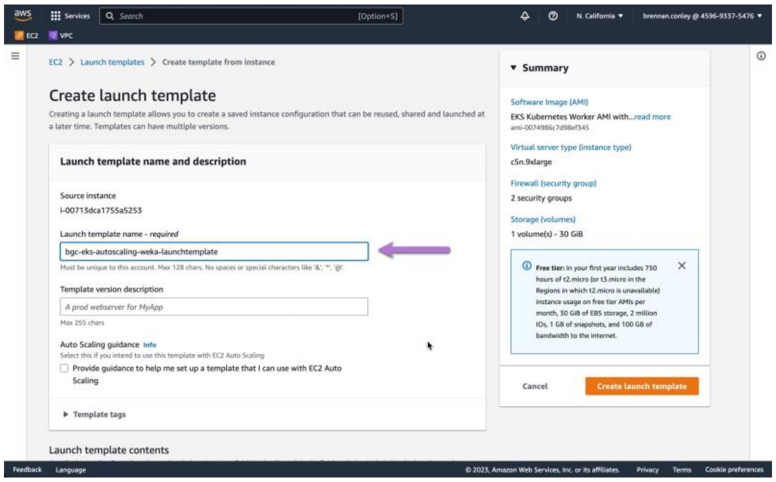
Instance ID	Public IPv4 address	Private IPv4 addresses
i-00713dca1755a5253	52.53.255.245 | open address	172.31.31.50
IPv6 address	**Instance state**	**Public IPv4 DNS**
–	Running	ec2-52-53-255-245.us-west-1.compute.amazonaws.com | open address

Next, from the *"Actions"* dropdown, select *"Image and Templates,"* then select *"Create template from instance."*



3. Modify the Launch Template parameters.

Enter a name for the Launch Template. The *"Template version description"* field is free text and can be used to describe the template's purpose, though it is not required.



EC2 > Launch templates > Create template from instance

Create launch template

Creating a launch template allows you to create a saved instance configuration that can be reused, shared and launched at a later time. Templates can have multiple versions.

Launch template name and description

Source instance
i-00713dca1755a5253

Launch template name - *required*
bgc-eks-autoscaling-weka-launchtemplate
Must be unique to this account. Max 128 chars. No spaces or special characters like '&', '*', '@'.

Template version description
A prod webserver for MyApp
Max 255 chars

Auto Scaling guidance Info
Select this if you intend to use this template with EC2 Auto Scaling
☐ Provide guidance to help me set up a template that I can use with EC2 Auto Scaling

▶ Template tags

Launch template contents

Summary

Software Image (AMI)
EKS Kubernetes Worker AMI with...read more
ami-0074986c7d98ef345

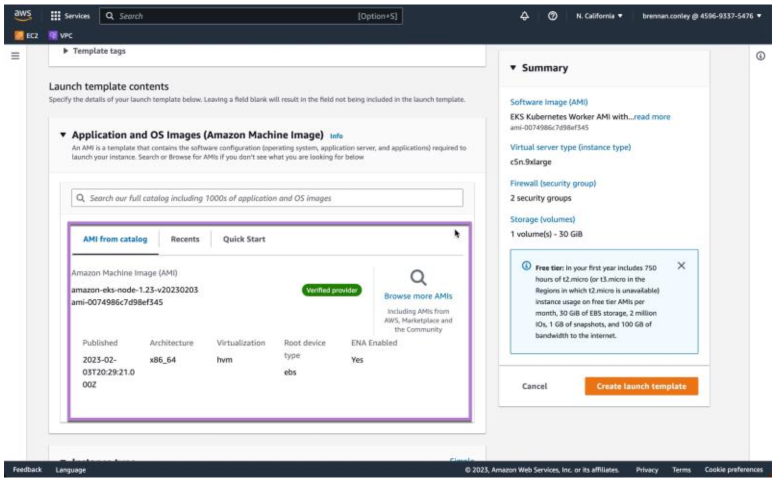
Virtual server type (instance type)
c5n.9xlarge

Firewall (security group)
2 security groups

Storage (volumes)
1 volume(s) - 30 GiB

Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 30 GiB of EBS storage, 2 million IOs, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

Under *"Application and OS Images"* retain the suggested AMI.



▶ Template tags

Launch template contents

Specify the details of your launch template below. Leaving a field blank will result in the field not being included in the launch template.

Application and OS Images (Amazon Machine Image) Info

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

Search our full catalog including 1000s of application and OS images

AMI from catalog | Recents | Quick Start

Amazon Machine Image (AMI)
amazon-eks-node-1.23-v20230203
ami-0074986c7d98ef345
Verified provider

Published	Architecture	Virtualization	Root device type	ENA Enabled
2023-02-03T20:29:21.000Z	x86_64	hvm	ebs	Yes

Summary

Software Image (AMI)
EKS Kubernetes Worker AMI with...read more
ami-0074986c7d98ef345

Virtual server type (instance type)
c5n.9xlarge

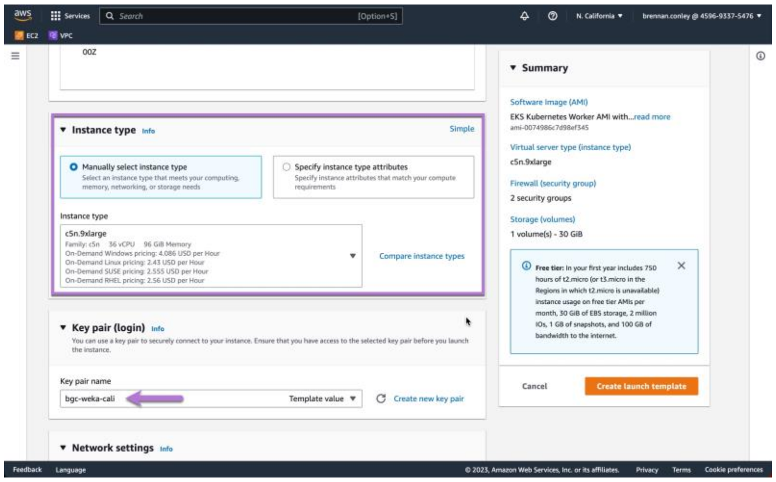
Firewall (security group)
2 security groups

Storage (volumes)
1 volume(s) - 30 GiB

Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 30 GiB of EBS storage, 2 million IOs, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

Services
Search
[Option+S]
N. California
brennan.conley @ 4596-9337-5476
EC2
VPC
Browse more AMIs
Including AMIs from AWS, Marketplace and the Community
Cancel
Create launch template
Feedback
Language
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Select the desired instance type to be deployed when using the Launch Template. Additionally, specify the desired AWS SSH key pair. To simplify, the key pair specified should be the same as the key pair used to deploy the Weka cluster.



00Z

Instance type Info — Simple

- (●) Manually select instance type — Select an instance type that meets your computing, memory, networking, or storage needs
- ( ) Specify instance type attributes — Specify instance attributes that match your compute requirements

Instance type
c5n.9xlarge
Family: c5n 36 vCPU 96 GiB Memory
On-Demand Windows pricing: 4.086 USD per Hour
On-Demand Linux pricing: 2.43 USD per Hour
On-Demand SUSE pricing: 2.555 USD per Hour
On-Demand RHEL pricing: 2.56 USD per Hour

Compare instance types

Key pair (login) Info
You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

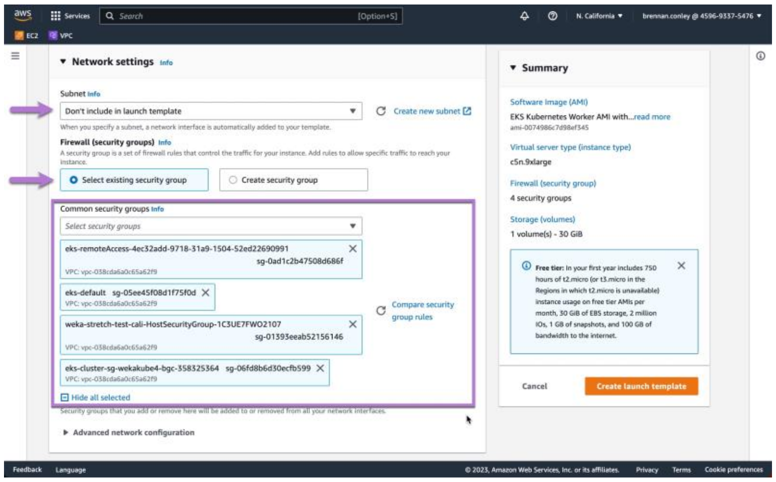
Key pair name: bgc-weka-cali — Template value
Create new key pair

Network settings Info

Summary
Software Image (AMI): EKS Kubernetes Worker AMI with...read more ami-0074986c7d98ef345
Virtual server type (instance type): c5n.9xlarge
Firewall (security group): 2 security groups
Storage (volumes): 1 volume(s) - 30 GiB

Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 30 GiB of EBS storage, 2 million IOs, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

For *"Network settings"* configure the desired security groups. The *Subnet* should be set to *"Don't include in launch template"* as the subnet details will be specified as part of the Autoscaling group. Keep in mind that the selected subnet should have access to the Weka cluster. The security group selection should include the security group for the EKS cluster management interfaces (created upon creation of EKS cluster), the Weka cluster HostSecurityGroup, the EKS remote access security group (if remote access is desired for the node group) and any other relevant security groups for the environment (application specific). Advanced network configuration can remain as default.



Network settings Info

Subnet Info: Don't include in launch template
Create new subnet
When you specify a subnet, a network interface is automatically added to your template.

Firewall (security groups) Info
A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

- (●) Select existing security group
- ( ) Create security group

Common security groups Info
Select security groups
- eks-remoteAccess-4ec32add-9718-31a9-1504-52ed22690991 sg-0ad1c2b47508d686f — VPC: vpc-038cda6a0c65a62f9
- eks-default sg-05ee45f08d1f75f0d — VPC: vpc-038cda6a0c65a62f9
- weka-stretch-test-cali-HostSecurityGroup-1C3UE7FWO2107 sg-01393eeab52156146 — VPC: vpc-038cda6a0c65a62f9
- eks-cluster-sg-wekakube4-bgc-358325364 sg-06fd8b6d30ecfb599 — VPC: vpc-038cda6a0c65a62f9

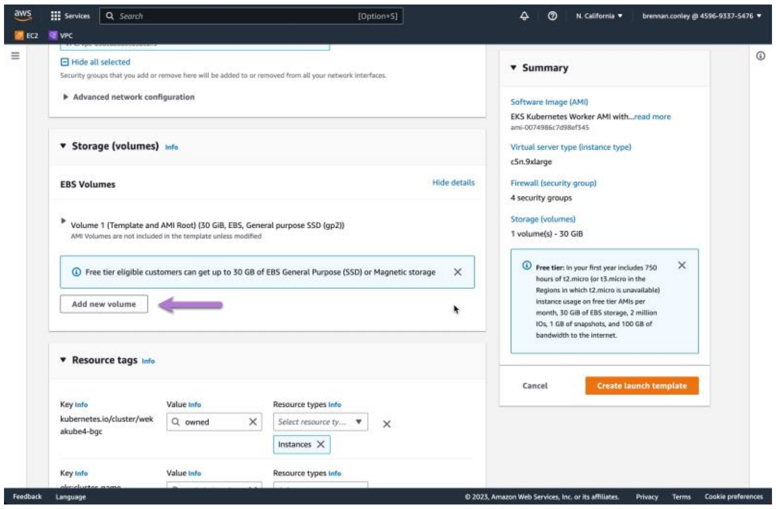
Hide all selected
Compare security group rules
Security groups that you add or remove here will be added to or removed from all your network interfaces.

Advanced network configuration

Summary
Software Image (AMI): EKS Kubernetes Worker AMI with...read more ami-0074986c7d98ef345
Virtual server type (instance type): c5n.9xlarge
Firewall (security group): 4 security groups
Storage (volumes): 1 volume(s) - 30 GiB

Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 30 GiB of EBS storage, 2 million IOs, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

Under *"Storage (volumes)"* EBS Volumes, select *"Add new volume."*


Storage (volumes) Info

EBS Volumes

Volume 1 (Template and AMI Root) (30 GiB, EBS, General purpose SSD (gp2))
AMI Volumes are not included in the template unless modified

Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage

Resource tags

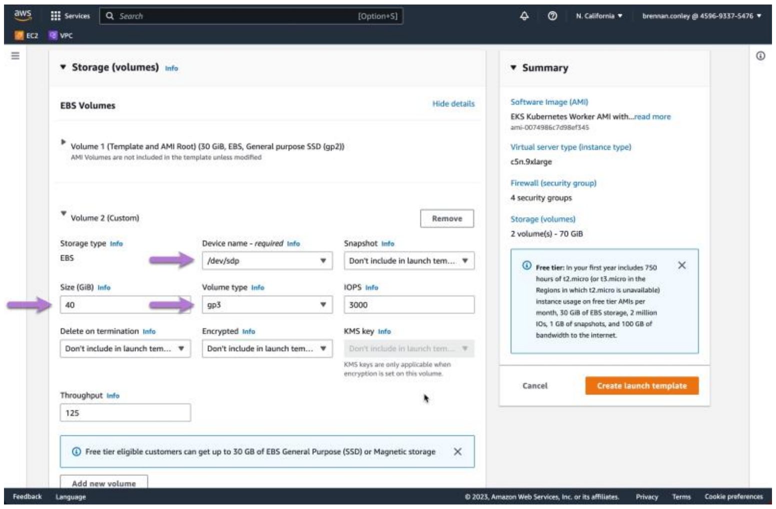
Key	Value	Resource types
kubernetes.io/cluster/wekakube4-bgc	owned	Instances

Summary
Software Image (AMI): EKS Kubernetes Worker AMI with...read more, ami-0074986c7d98ef345
Virtual server type (instance type): c5n.9xlarge
Firewall (security group): 4 security groups
Storage (volumes): 1 volume(s) - 30 GiB

Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 30 GiB of EBS storage, 2 million IOs, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

Services
Search
[Option+S]
N. California
brennan.conley @ 4596-9337-5476
EC2
VPC
Hide all selected
Security groups that you add or remove here will be added to or removed from all your network interfaces.
Advanced network configuration
Hide details
Add new volume
Select resource ty...
Cancel
Create launch template
Feedback
Language
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Create an additional small EBS volume (40GB will be sufficient) for the Weka client. The EBS volume will only hold the Weka software installation and debugging logs. Set the *device name* to `/dev/sdp` and the *volume type* to gp3. *Do not* modify the existing EBS volume (listed as Volume 1) which is configured by default.


Storage (volumes) Info

EBS Volumes

Volume 1 (Template and AMI Root) (30 GiB, EBS, General purpose SSD (gp2))
AMI Volumes are not included in the template unless modified

Volume 2 (Custom)

Storage type: EBS
Device name - *required*: /dev/sdp
Snapshot: Don't include in launch tem...
Size (GiB): 40
Volume type: gp3
IOPS: 3000
Delete on termination: Don't include in launch tem...
Encrypted: Don't include in launch tem...
KMS key: Don't include in launch tem...
KMS keys are only applicable when encryption is set on this volume.
Throughput: 125

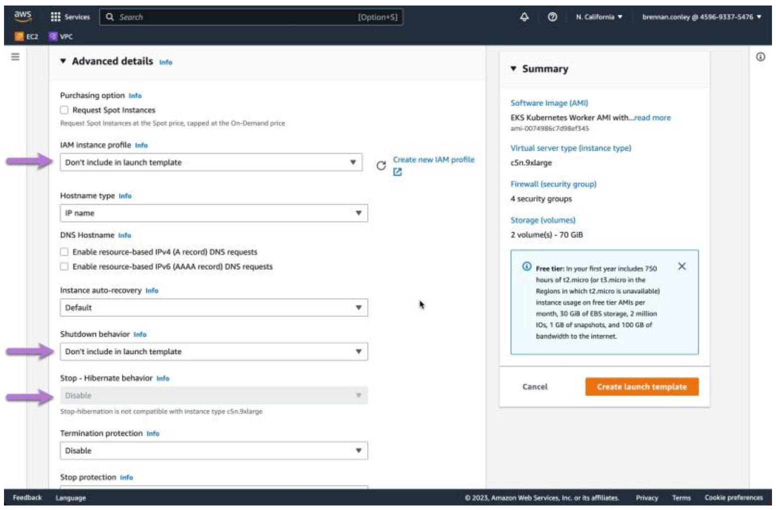
Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage

Summary
Software Image (AMI): EKS Kubernetes Worker AMI with...read more, ami-0074986c7d98ef345
Virtual server type (instance type): c5n.9xlarge
Firewall (security group): 4 security groups
Storage (volumes): 2 volume(s) - 70 GiB

Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 30 GiB of EBS storage, 2 million IOs, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

Leave *"Resource tags"* as default and do not modify any values.

Expand *"Advanced details"* and configure the *IAM instance profile* to *"Don't include in launch template."* Additionally, configure both *Shutdown behavior* and *Stop - Hibernate behavior* to *"Don't include in launch template."* Some instances do not allow *Stop - Hibernate behavior* to be modified. In these cases, the field will be disabled and default should be accepted. All additional options can be left as default until *User data - optional* is reached.



▼ Advanced details Info

Purchasing option Info
☐ Request Spot Instances
Request Spot Instances at the Spot price, capped at the On-Demand price

IAM instance profile Info
Don't include in launch template
Create new IAM profile

Hostname type Info
IP name

DNS Hostname Info
☐ Enable resource-based IPv4 (A record) DNS requests
☐ Enable resource-based IPv6 (AAAA record) DNS requests

Instance auto-recovery Info
Default

Shutdown behavior Info
Don't include in launch template

Stop - Hibernate behavior Info
Disable
Stop-hibernation is not compatible with instance type c5n.9xlarge

Termination protection Info
Disable

Stop protection Info

▼ Summary

Software Image (AMI)
EKS Kubernetes Worker AMI with...read more
ami-0074986c7d98ef345

Virtual server type (instance type)
c5n.9xlarge

Firewall (security group)
4 security groups

Storage (volumes)
2 volume(s) - 70 GiB

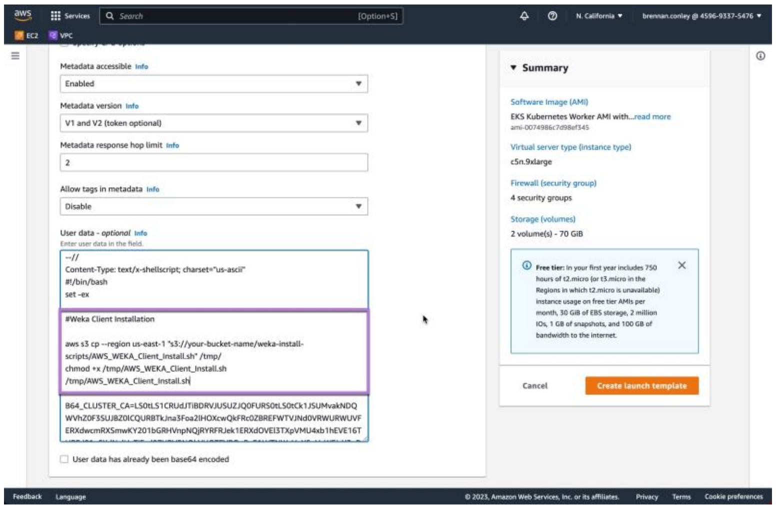
Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 30 GiB of EBS storage, 2 million IOs, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

Cancel | Create launch template

Finally, under *User data - optional* modify the script to include the code snippet below. Before copying and pasting, be sure to update the S3 URL to reflect your S3 bucket name and directory of the stored install script.

```
#Weka Client Installation

aws s3 cp --region us-east-1 "s3://your-bucket-name/weka-install-scripts/AWS_WEKA_Client_In
stall.sh" /tmp/
chmod +x /tmp/AWS_WEKA_Client_Install.sh
/tmp/AWS_WEKA_Client_Install.sh
```

The code should be pasted *after* `set -ex` and before `B64_CLUSTER_CA=` in the existing user data. An example is shown below.



Metadata accessible Info
Enabled

Metadata version Info
V1 and V2 (token optional)

Metadata response hop limit Info
2

Allow tags in metadata Info
Disable

User data - *optional* Info
Enter user data in the field.

```
--//
Content-Type: text/x-shellscript; charset="us-ascii"
#!/bin/bash
set -ex

#Weka Client Installation

aws s3 cp --region us-east-1 "s3://your-bucket-name/weka-install-
scripts/AWS_WEKA_Client_Install.sh" /tmp/
chmod +x /tmp/AWS_WEKA_Client_Install.sh
/tmp/AWS_WEKA_Client_Install.sh

B64_CLUSTER_CA=LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCk1JSUMvakNDQ
WVhZ0F3SUJBZ0lCQURBTkJna3Foa2lHOXcwQkFRc0ZBREFWTVJNd0VRWURWUVF
ERXdwcmRXSmwKY201bGRHVnpNQjRYRFRJek1ERXdOVEl3TXpVMU4xb1hEVE16T
```

☐ User data has already been base64 encoded

▼ Summary

Software Image (AMI)
EKS Kubernetes Worker AMI with...read more
ami-0074986c7d98ef345

Virtual server type (instance type)
c5n.9xlarge

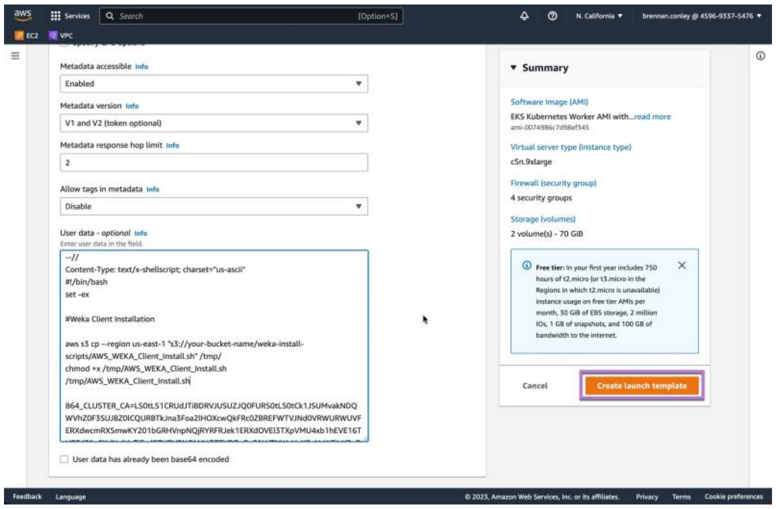
Firewall (security group)
4 security groups

Storage (volumes)
2 volume(s) - 70 GiB

Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 30 GiB of EBS storage, 2 million IOs, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

Cancel | Create launch template

To complete the Launch Template configuration, select *"Create launch template."*


Metadata accessible: Enabled

Metadata version: V1 and V2 (token optional)

Metadata response hop limit: 2

Allow tags in metadata: Disable

User data - *optional*
Enter user data in the field.

```
--//
Content-Type: text/x-shellscript; charset="us-ascii"
#!/bin/bash
set -ex

#Weka Client Installation

aws s3 cp --region us-east-1 "s3://your-bucket-name/weka-install-
scripts/AWS_WEKA_Client_Install.sh" /tmp/
chmod +x /tmp/AWS_WEKA_Client_Install.sh
/tmp/AWS_WEKA_Client_Install.sh

B64_CLUSTER_CA=LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCk1JSUMvakNDQ
WVhZ0F3SUJBZ0lCQURBTkJna3Foa2lHOXcwQkFRc0ZBREFWTVJNd0VRWURWUVF
ERXdwcmRXSmwKY201bGRHVnpNQjRYRFRJek1ERXdOVEl3TXpVMU4xb1hEVE16T
```

☐ User data has already been base64 encoded

Summary

Software Image (AMI): EKS Kubernetes Worker AMI with...read more
ami-0074986c7d98ef345

Virtual server type (instance type): c5n.9xlarge

Firewall (security group): 4 security groups

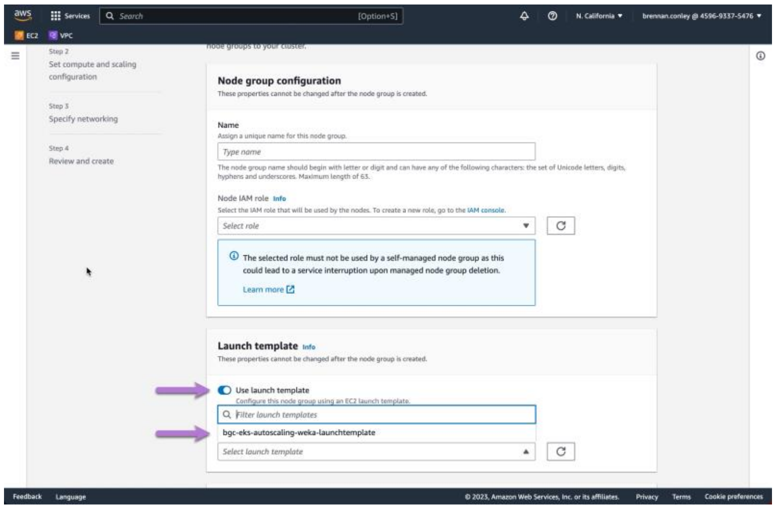
Storage (volumes): 2 volume(s) - 70 GiB

Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 30 GiB of EBS storage, 2 million IOs, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

The Launch Template is now created.

4. Create an autoscaling node group by using the Launch Template

To create a node group with the Weka client pre-installed in preparation for autoscaling node groups, you can follow the instructions provided earlier in this documentation under "Creating node groups - non-autoscaling" with one small modification. When configuring the node group, under "Launch template" ensure *"Use launch template"* is toggled on as shown below. Select the newly created Launch Template from the "Launch template name" drop down as shown.



Node group configuration
These properties cannot be changed after the node group is created.

Name
Assign a unique name for this node group.
Type name
The node group name should begin with letter or digit and can have any of the following characters: the set of Unicode letters, digits, hyphens and underscores. Maximum length of 63.

Node IAM role
Select the IAM role that will be used by the nodes. To create a new role, go to the IAM console.
Select role

The selected role must not be used by a self-managed node group as this could lead to a service interruption upon managed node group deletion.
Learn more

Launch template
These properties cannot be changed after the node group is created.

Use launch template
Configure this node group using an EC2 launch template.
Filter launch templates
bgc-eks-autoscaling-weka-launchtemplate
Select launch template

Proceed through the remainder of the node group configuration as shown before in the "Creating node groups - non-autoscaling" section. Once the node group has been configured and deployed, the Weka CSI driver can be installed and deployment of applications can begin.

Installing the WEKA CSI driver

Instructions for installing the Weka CSI driver can be found on docs.weka.io in the appendix, linked to here.