**TABLE OF CONTENTS**

[**1.** **Create IAM Role** 2](#_Toc182837660)

[1.1. EFS Role 2](#_Toc182837661)

[1.2. EFS Role Trust Relationships 4](#_Toc182837662)

[**2.** **Update KMS Key JSON Policy** 4](#_Toc182837663)

[**3.** **Attach IAM Role to EKS Add-Ons** 5](#_Toc182837664)

[**4.** **VPC Endpoint** 5](#_Toc182837665)

[4.1. EC2 VPC Endpoint 5](#_Toc182837666)

[**5.** **EFS Creation into AWS Console** 8](#_Toc182837667)

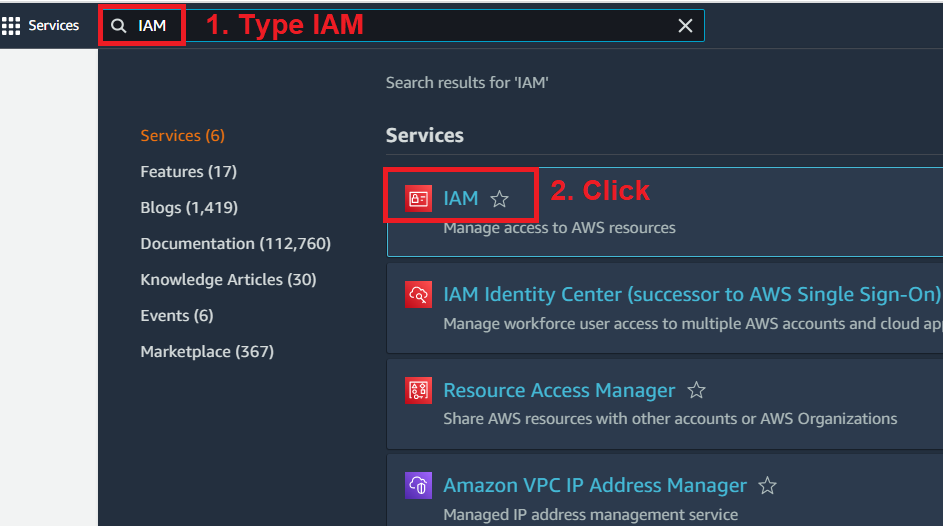
[**6.** **EFS Pods** 9](#_Toc182837668)

# **Create IAM Role**

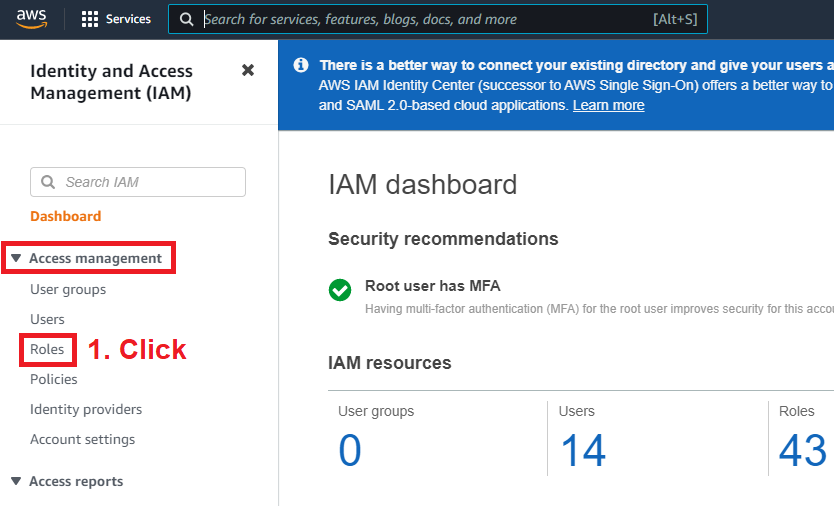
* Create the EFS role and update the trust.

## EFS Role

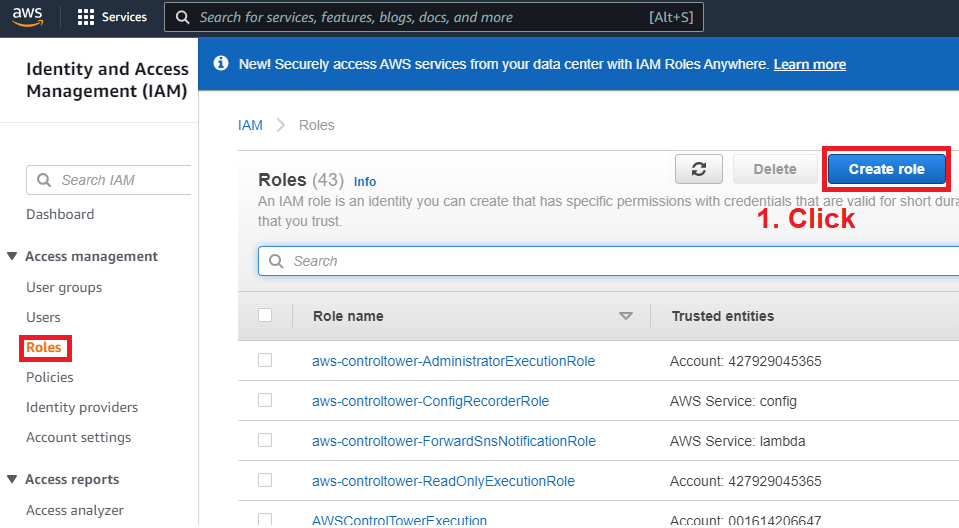
* Login into AWS Console 🡪 Type **IAM** in search 🡪 Click **IAM**



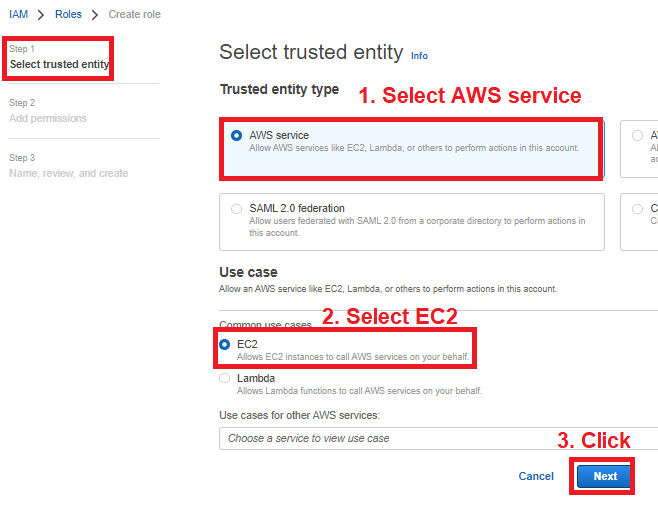
* Click on **Roles** under Access management



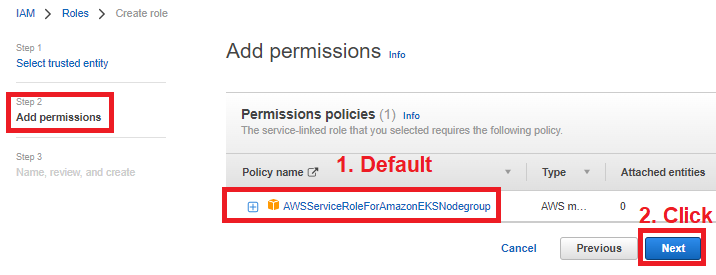
* Click on **Create Role** Right Top



* Select **AWS service** 🡪 Select **EC2**



* On Add Permission 🡪 Don’t Change Default 🡪 Click Next



* Select the following Policy as below 🡪 Click **Next**

[AmazonEFSCSIDriverPolicy](https://us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/policies/details/arn%3Aaws%3Aiam%3A%3Aaws%3Apolicy%2Fservice-role%2FAmazonEFSCSIDriverPolicy)

[AmazonEC2ContainerRegistryReadOnly](https://us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/policies/details/arn%3Aaws%3Aiam%3A%3Aaws%3Apolicy%2FAmazonEC2ContainerRegistryReadOnly) 🡪 Optional

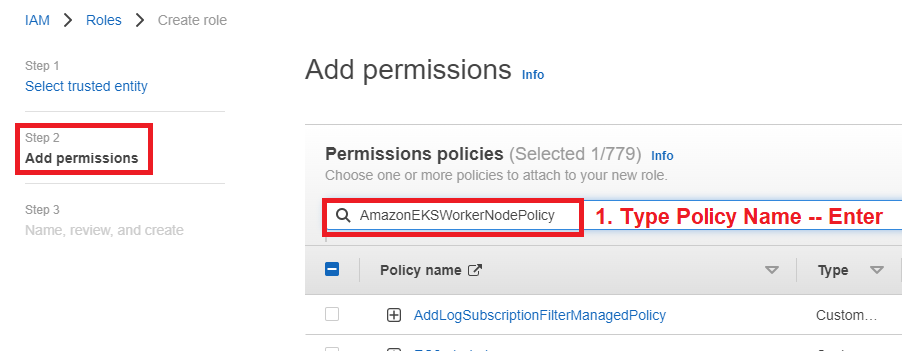
[AmazonEBSCSIDriverPolicy](https://us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/policies/details/arn%3Aaws%3Aiam%3A%3Aaws%3Apolicy%2Fservice-role%2FAmazonEBSCSIDriverPolicy) 🡪 Optional

[AmazonEKS\_CNI\_Policy](https://us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/policies/details/arn%3Aaws%3Aiam%3A%3Aaws%3Apolicy%2FAmazonEKS_CNI_Policy) 🡪 Optional

[AmazonEKSWorkerNodePolicy](https://us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/policies/details/arn%3Aaws%3Aiam%3A%3Aaws%3Apolicy%2FAmazonEKSWorkerNodePolicy) 🡪 Optional

[AmazonSSMManagedInstanceCore](https://us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/policies/details/arn%3Aaws%3Aiam%3A%3Aaws%3Apolicy%2FAmazonSSMManagedInstanceCore) 🡪 Optional

[CloudWatchFullAccess](https://us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/policies/details/arn%3Aaws%3Aiam%3A%3Aaws%3Apolicy%2FCloudWatchFullAccess) 🡪 Optional



* Add Below KMS Key Policy in Above Role



## EFS Role Trust Relationships

* Select the following 5 Policy as below 🡪 Click **Next**



{

"Version": "2012-10-17",

"Statement": [

{

"Effect": "Allow",

"Principal": {

"Service": "ec2.amazonaws.com",

"AWS": "arn:aws:iam::385089911239:role/hbl-aws-cam-role-eks-workernode-lentra-prod"

},

"Action": "sts:AssumeRole"

},

{

"Effect": "Allow",

"Principal": {

"Federated": "arn:aws:iam::385089911239:oidc-provider/oidc.eks.ap-south-1.amazonaws.com/id/A6A20B8F7F1690F755A1D372370FF5C4"

},

"Action": "sts:AssumeRoleWithWebIdentity",

"Condition": {

"StringEquals": {

"oidc.eks.ap-south-1.amazonaws.com/id/A6A20B8F7F1690F755A1D372370FF5C4:sub": [

"system:serviceaccount:kube-system:efs-csi-controller-sa",

"system:serviceaccount:kube-system:ebs-csi-controller-sa",

"system:serviceaccount:kube-system:efs-csi-node-sa"

],

"oidc.eks.ap-south-1.amazonaws.com/id/A6A20B8F7F1690F755A1D372370FF5C4:aud": "sts.amazonaws.com"

}

}

}

]

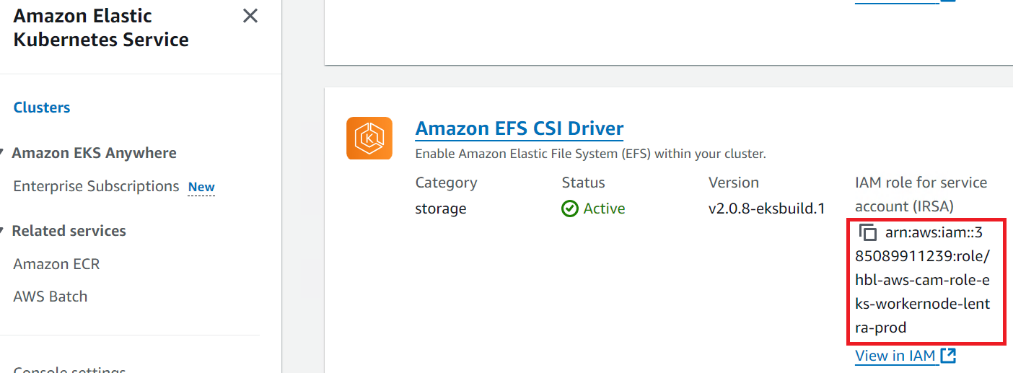
}

# **Update KMS Key JSON Policy**

* Raise a request to create KMS Key Sample JSON attached.



# **Attach IAM Role to EKS Add-Ons**



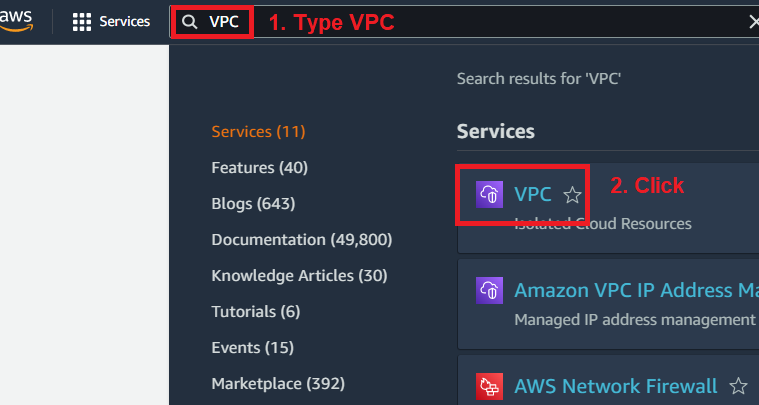
# **VPC Endpoint**

* Create the Following **VPC** **EndPoints** with SecurityGroup(443 Must Allow).

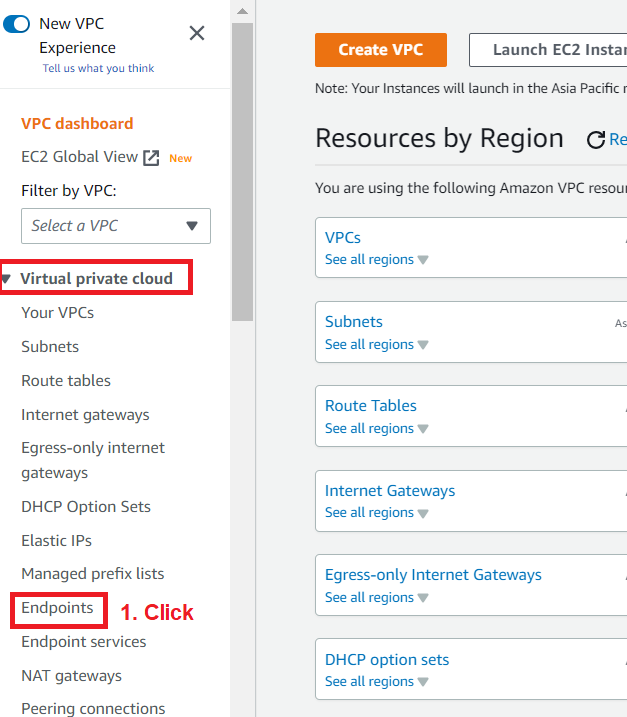
com.amazonaws.ap-south-1.elasticfilesystem

## EC2 VPC Endpoint

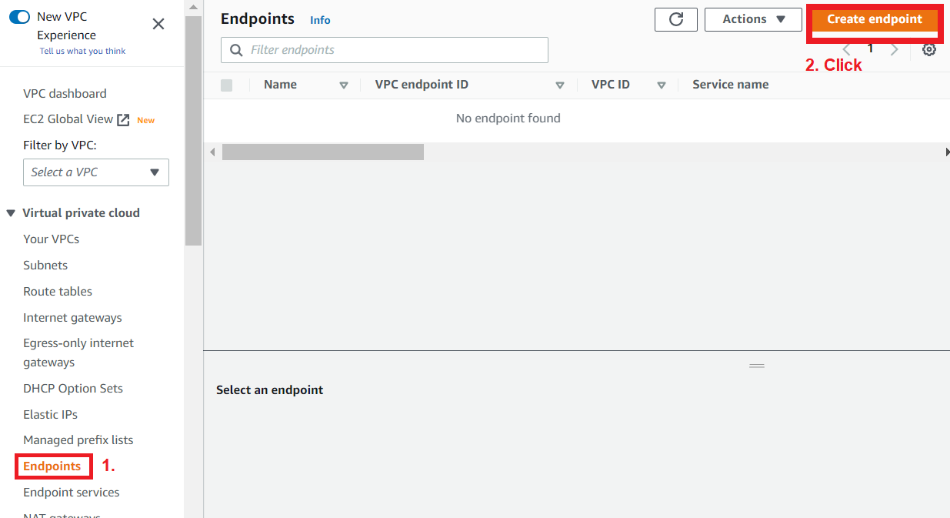
* Login into AWS Console 🡪 Type VPC in search 🡪 Click on VPC



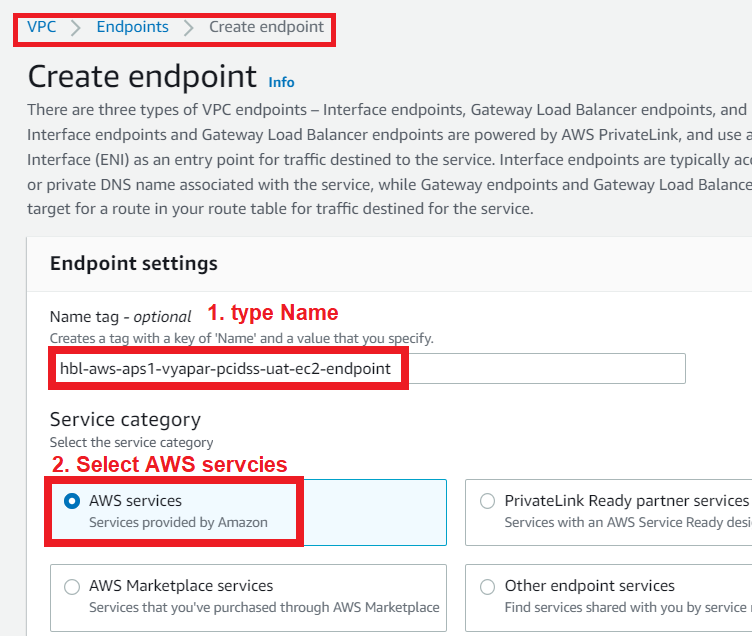
* Click on **Endpoints** under Virtual private cloud



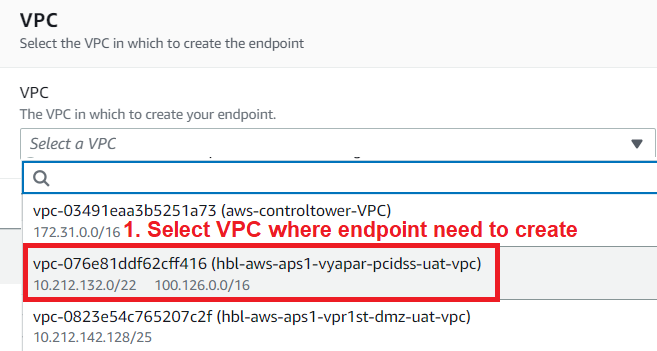
* Click on **Create endpoint** on right top



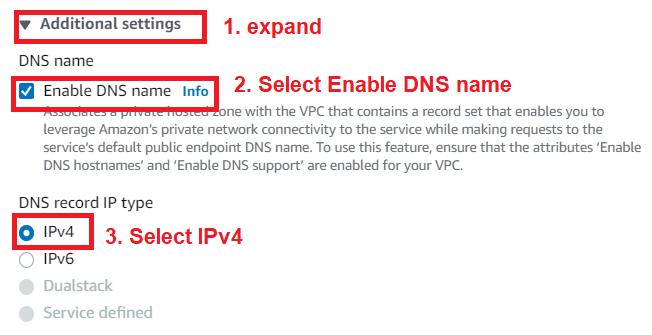
* Type the Name 🡪 Select AWS services



* Type **elastic** in Services 🡪 Select **com.amazonaws.ap-south-1.elasticfilesystem**
* Select the VPC in which endpoint need to create – Example – pcidss



* Expand – **Additional Setting** 🡪 Select **Enable DNS name** 🡪 Select **IPv4**.

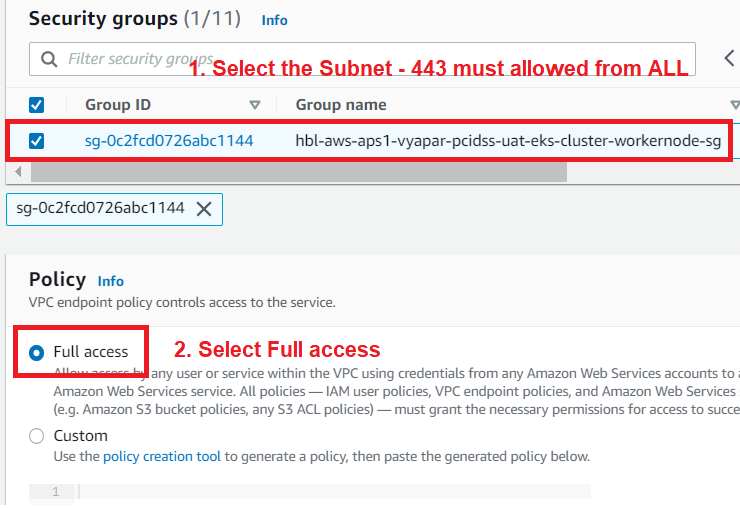


* Select **INFRA Subnet** as Availability Zone from Subnet where endpoints need to attach.

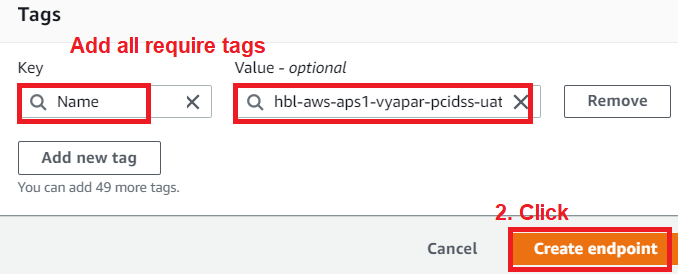
Graphical user interface, text, application, email

Description automatically generated

* Select the Security Group – 443 must allow from ALL



* Type All require tags 🡪 Click **Create endpoint**



# **EFS Creation into AWS Console**

* Use following TFE code create EFS



* Following **File System Policy** must be requiring code create EFS

{

"Version": "2012-10-17",

"Statement": [

{

"Sid": "EFS-Allow",

"Effect": "Allow",

"Principal": {

"AWS": "\*"

},

"Action": [

"elasticfilesystem:ClientWrite",

"elasticfilesystem:ClientRootAccess",

"elasticfilesystem:ClientMount"

],

"Resource": "arn:aws:elasticfilesystem:ap-south-1:385089911239:file-system/fs-0400ac090973d0a92"

},

{

"Sid": "NonSecureTransport",

"Effect": "Deny",

"Principal": {

"AWS": "\*"

},

"Action": "\*",

"Resource": "arn:aws:elasticfilesystem:ap-south-1:385089911239:file-system/fs-0400ac090973d0a92",

"Condition": {

"Bool": {

"aws:SecureTransport": "false"

}

}

}

]

}

# **EFS Pods**

* Use following TFE code create EFS Pods

# vi efs.yaml

apiVersion: storage.k8s.io/v1

kind: StorageClass

metadata:

name: efs-sc

provisioner: efs.csi.aws.com

parameters:

directoryPerms: "700"

fileSystemId: fs-0400ac090973d0a92

provisioningMode: efs-ap

basePath: "/"

reclaimPolicy: Retain

volumeBindingMode: WaitForFirstConsumer

* Use following TFE code create EFS Pods

# kubectl apply -f efs.yaml