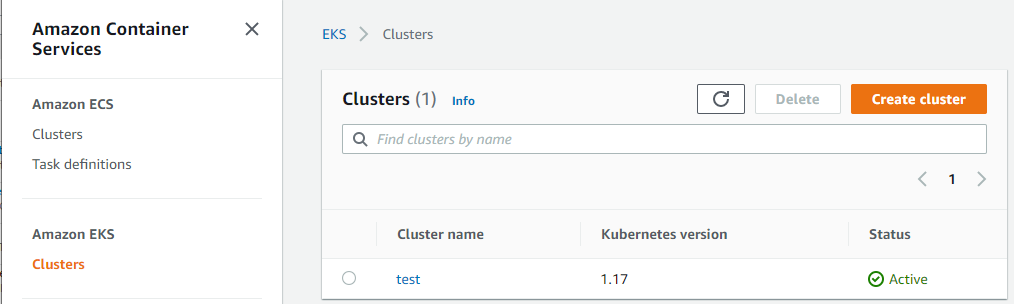
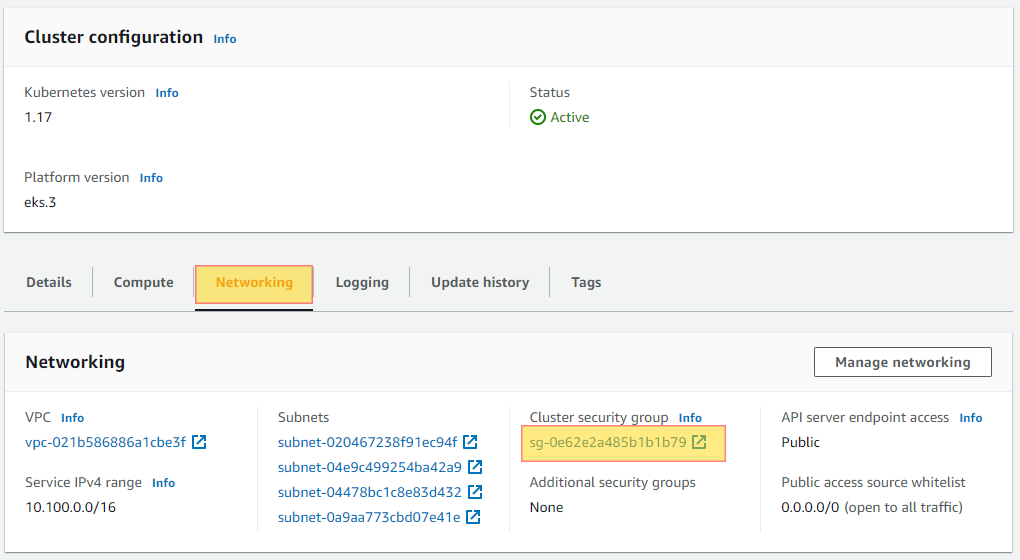
AWS EKS security groups allow incoming traffic only on TCP port 443

Steps test:

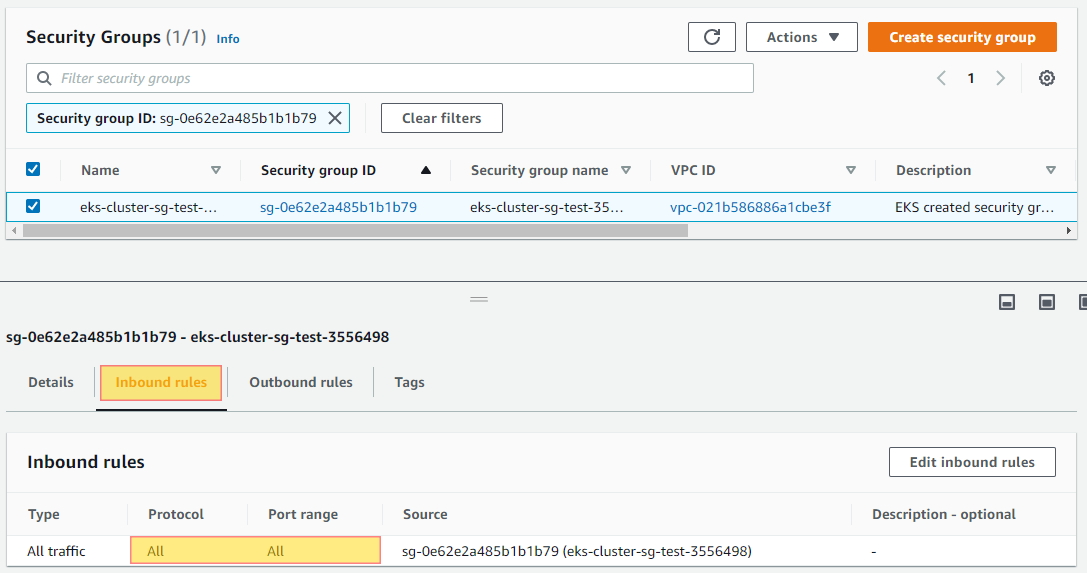
1. Login into your AWS account
2. Navigate to the ECS service at: <https://console.aws.amazon.com/ecs>
3. On the left hand panel select **Clusters** under **Amazon EKS**.



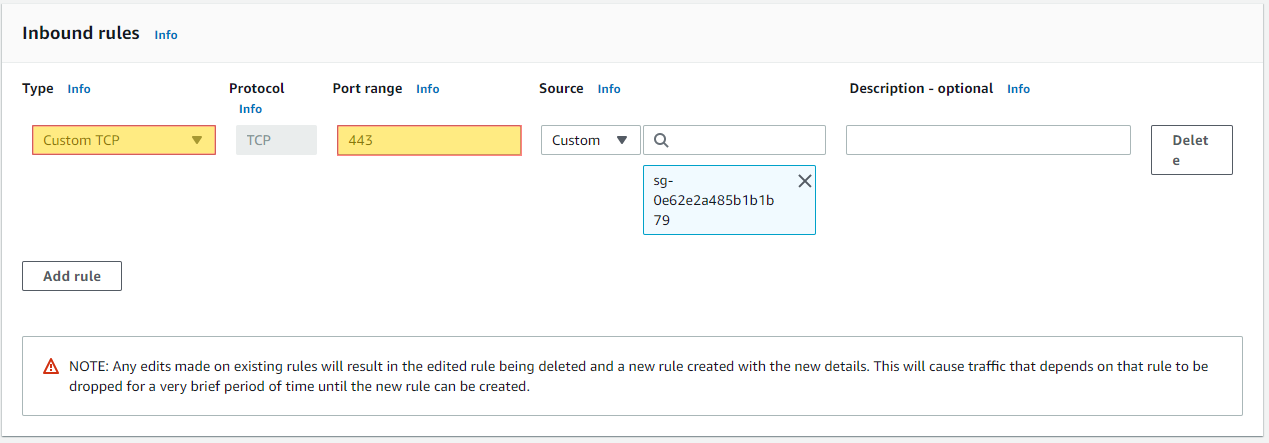
1. Select the EKS cluster in order to go into the **Cluster configuration** page.
2. Select the **Networking** tab and select the hyperlink for **Cluster security group**.



1. This will open a new browser tab taking you directly to the **Security group**.
2. Select the **Security group** that has been filtered,
3. Select the **Inbound rules** tab and validate if **Port range** has anything other than **443** listed.



1. Select **Edit inbound rules** and change the security group to only allow inbound on port **443**.



Envelope encryption for EKS Kubernetes Secrets is enabled using Amazon KMS

Test steps:

1. Open the Amazon EKS console at <https://console.aws.amazon.com/eks/home#/clusters>.
2. Choose the cluster that you want to add KMS encryption to.
3. Choose the **Overview** tab (this is selected by default).
4. Scroll down to the **Secrets encryption** section and choose **Enable**.
5. Select a key from the dropdown list and choose the **Enable** button. If no keys are listed, you must create one first. For more information, see [Creating keys](https://docs.aws.amazon.com/kms/latest/developerguide/create-keys.html)
6. Choose the **Confirm** button to use the chosen key.

EKS control plane logging is enabled for your Amazon EKS clusters

Test steps:

1. Open the [Amazon EKS console](https://console.aws.amazon.com/eks/home#/clusters).
2. Choose the name of the cluster to display your cluster information.
3. Choose the **Logging** tab and choose **Manage logging**.
4. For each individual log type, choose whether the log type should be **Enabled** or **Disabled**. By default, each log type is **Disabled**.
5. Choose **Save changes** to finish.

The latest version of Kubernetes is installed on your Amazon EKS clusters

Test steps:

1. Open the Amazon EKS console at <https://console.aws.amazon.com/eks/home#/clusters>.
2. Choose the name of the Amazon EKS cluster to update and choose **Update cluster version**.
3. For **Kubernetes version**, select the version to update your cluster to and choose **Update**.
4. For **Cluster name**, enter the name of your cluster and choose **Confirm**.

Amazon EKS configuration changes are monitored.

Test steps:

Using tool like Trend Micro Cloud One Conformity

<https://www.trendmicro.com/cloudoneconformity/knowledge-base/aws/EKS/configuration-changes.html>