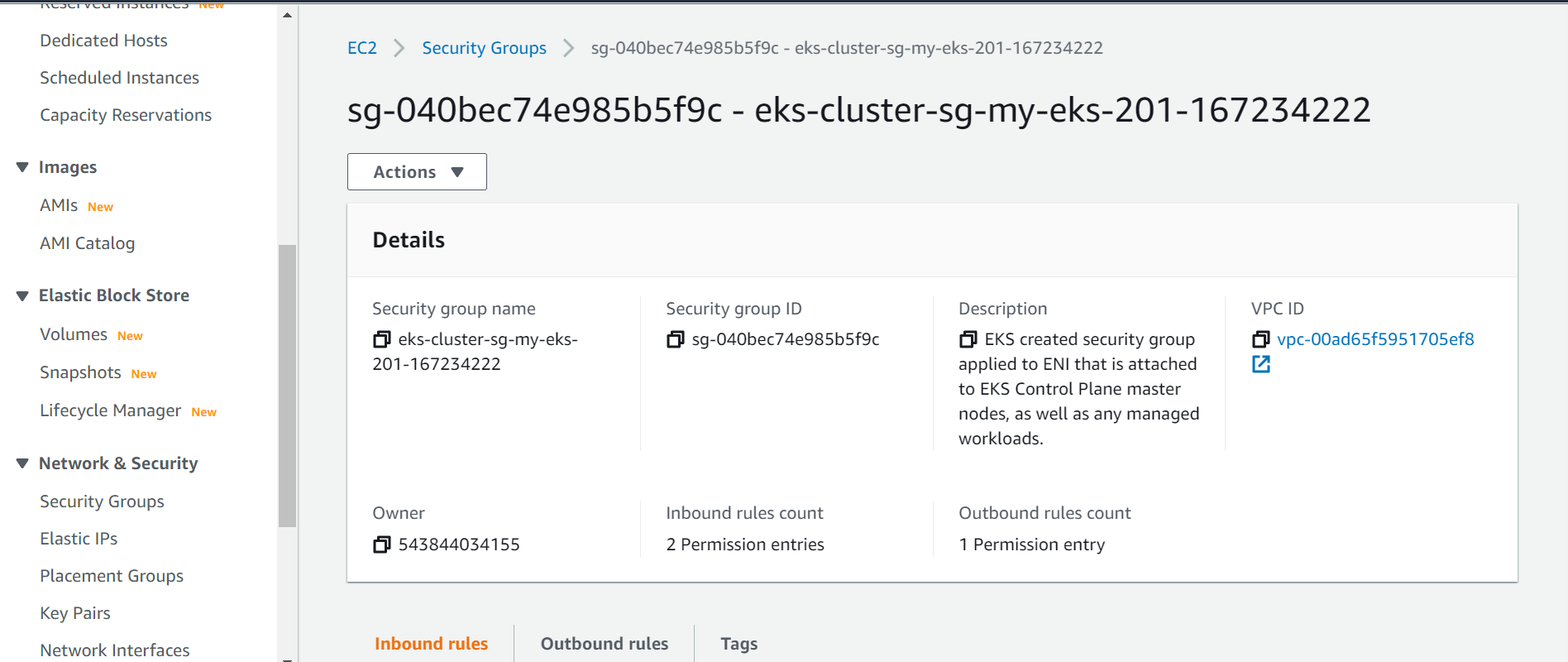
Amazon EKS creates an endpoint for any managed Kubernetes API server to communicate with the cluster. By default, this API server endpoint is public to the internet. Access to it should be regulated using AWS IAM and native Kubernetes RBAC.



Creating restrictions to allow only necessary service-to-service and cluster egress connections decreases the number of potential targets for malicious or misconfigured pods and limits their ability to exploit the cluster resources. AWS Security groups[1](https://docs.aws.amazon.com/eks/latest/userguide/security-groups-for-pods.html) for pods integrate Amazon EC2 security groups with Kubernetes pods. You can use Amazon EC2 security groups to define rules that allow inbound and outbound network traffic to and from pods that you deploy to nodes running on many Amazon EC2 instance types and Fargate

