Project by Himani Arora - ELK on Amazon EKS

aws ec2 create-key-pair --key-name ELKpoc.pem --query 'KeyMaterial' --output text > ELKpoc.pem

aws cloudformation create-stack --stack-name my-eks-cluster --template-body file://cf-template.yaml --capabilities CAPABILITY_IAM --parameters ParameterKey=KeyName,ParameterValue=ELKpoc.pem

```
himaniarora@DESKTOP-MKJ MINGW64 ~/.kube
$ aws eks update-kubeconfig --name eks-cluster --region eu-west-1
Updated context arn:aws:eks:eu-west-1:891497802633:cluster/eks-cluster in C:\Users\himaniaro\.kube\config

himaniarora@DESKTOP-MKJ MINGW64 ~/.kube
$ kubectl get namespaces
NAME              STATUS   AGE
default           Active   6m39s
kube-node-lease   Active   6m39s
kube-public       Active   6m39s
kube-system       Active   6m39s

himaniarora@DESKTOP-MKJ MINGW64 ~/.kube
$ kubectl create namespace elk
namespace/elk created

himaniarora@DESKTOP-MKJ MINGW64 ~/.kube
$ helm repo add aws-ebs-csi-driver https://kubernetes-sigs.github.io/aws-ebs-csi-driver
"aws-ebs-csi-driver" has been added to your repositories

himaniarora@DESKTOP-MKJ MINGW64 ~/.kube
$ helm repo update
Hang tight while we grab the latest from your chart repositories...
...Successfully got an update from the "aws-ebs-csi-driver" chart repository
...Successfully got an update from the "elastic" chart repository
Update Complete. ⎈Happy Helming!⎈

himaniarora@DESKTOP-MKJ MINGW64 ~/.kube
$ helm install aws-ebs-csi-driver aws-ebs-csi-driver/aws-ebs-csi-driver --namespace kube-system
NAME: aws-ebs-csi-driver
LAST DEPLOYED: Thu Jun 20 02:09:14 2024
NAMESPACE: kube-system
STATUS: deployed
REVISION: 1
NOTES:
To verify that aws-ebs-csi-driver has started, run:

    kubectl get pod -n kube-system -l "app.kubernetes.io/name=aws-ebs-csi-driver,app.kubernetes.io/instance=aws-ebs-csi-driver"

NOTE: The [CSI Snapshotter](https://github.com/kubernetes-csi/external-snapshotter) controller and CRDs will no longer be installed as part of this chart and moving forward will be a prerequisite of using the s
nap shotting functionality.
```

```
himaniaro@GGL7HM2 MINGW64 ~/.kube
$  kubectl get pods -n kube-system -l app=ebs-csi-controller
NAME                                 READY   STATUS    RESTARTS   AGE
ebs-csi-controller-f75fcfb49-hn8rn   5/5     Running   0          31s
ebs-csi-controller-f75fcfb49-x2nm6   5/5     Running   0          31s

himaniaro@GGL7HM2 MINGW64 ~/.kube
$  kubectl get pods -n kube-system -l app=ebs-csi-node
NAME                 READY   STATUS    RESTARTS   AGE
ebs-csi-node-6jjbc   3/3     Running   0          57s
ebs-csi-node-8sg95   3/3     Running   0          57s
ebs-csi-node-h6xqg   3/3     Running   0          57s

himaniaro@GGL7HM2 MINGW64 ~/.kube
$  helm repo add elastic https://helm.elastic.co
"elastic" already exists with the same configuration, skipping

himaniaro@GGL7HM2 MINGW64 ~/.kube
$ helm repo update
Hang tight while we grab the latest from your chart repositories...
...Successfully got an update from the "aws-ebs-csi-driver" chart repository
...Successfully got an update from the "elastic" chart repository
Update Complete. ⎈Happy Helming!⎈

himaniaro@GGL7HM2 MINGW64 ~/.kube
$  helm install elasticsearch elastic/elasticsearch --namespace elk
NAME: elasticsearch
LAST DEPLOYED: Thu Jun 20 02:12:26 2024
NAMESPACE: elk
STATUS: deployed
REVISION: 1
NOTES:
1. Watch all cluster members come up.
  $ kubectl get pods --namespace=elk -l app=elasticsearch-master -w
2. Retrieve elastic user's password.
  $ kubectl get secrets --namespace=elk elasticsearch-master-credentials -ojsonpath='{.data.password}' | base64 -d
3. Test cluster health using Helm test.
  $ helm --namespace=elk test elasticsearch

himaniaro@GGL7HM2 MINGW64 ~/.kube
$ kubectl get pods -n=elk
NAME                     READY   STATUS    RESTARTS   AGE
elasticsearch-master-0   0/1     Pending   0          30s
elasticsearch-master-1   0/1     Pending   0          30s
elasticsearch-master-2   0/1     Pending   0          30s
```

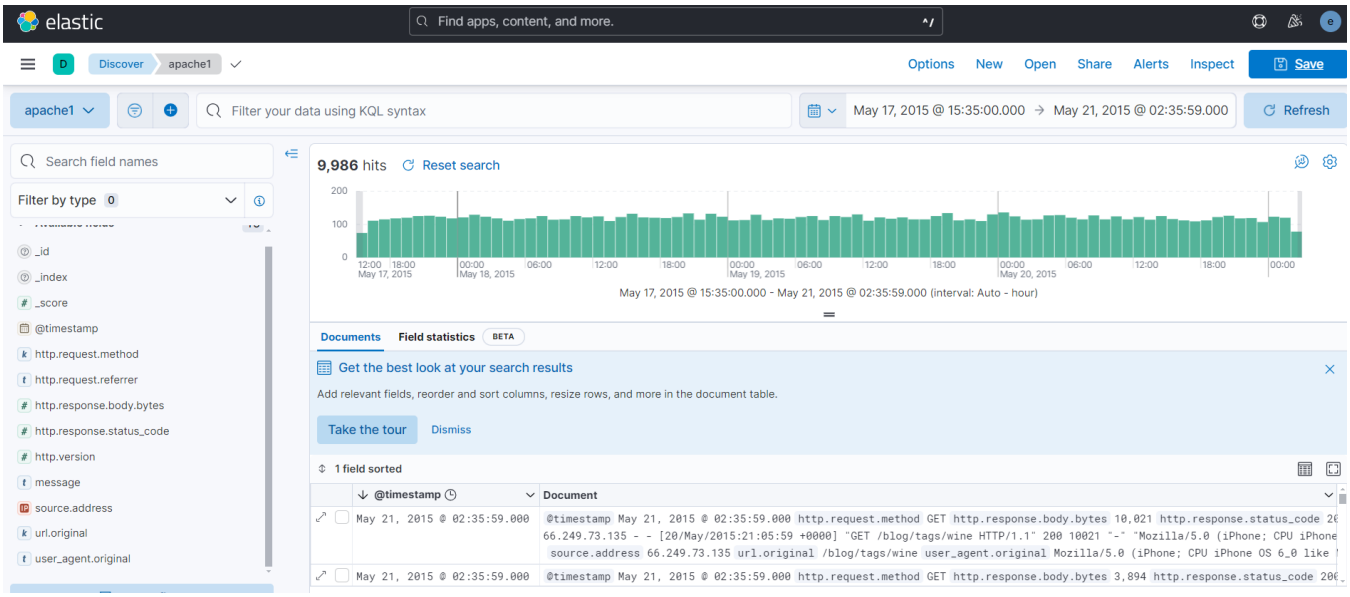
```
himaniaro@GGL7HM2 MINGW64 ~/.kube
$ aws eks list-nodegroups --cluster-name eks-cluster
{
    "nodegroups": [
        "eks-node-group"
    ]
}

himaniaro@GGL7HM2 MINGW64 ~/.kube
$ aws eks describe-nodegroup --cluster-name node-group --nodegroup-name eks-node-group

An error occurred (ResourceNotFoundException) when calling the DescribeNodegroup operation: No cluster found for name: node-group.

himaniaro@GGL7HM2 MINGW64 ~/.kube
$ aws eks describe-nodegroup --cluster-name eks-cluster --nodegroup-name eks-node-group
{
    "nodegroup": {
        "nodegroupName": "eks-node-group",
        "nodegroupArn": "arn:aws:eks:eu-west-1:891497802633:nodegroup/eks-cluster/eks-node-group/28c81919-ea5c-0fc0-71be-b0101a17f871",
        "clusterName": "eks-cluster",
        "version": "1.30",
        "releaseVersion": "1.30.0-20240605",
        "createdAt": "2024-06-20T02:02:57.586000+05:30",
        "modifiedAt": "2024-06-20T02:13:22.559000+05:30",
        "status": "ACTIVE",
        "capacityType": "ON_DEMAND",
        "scalingConfig": {
            "minSize": 1,
            "maxSize": 3,
            "desiredSize": 3
```

```
himaniarr@GGL7HM2 MINGW64 ~/.kube
$ aws iam attach-role-policy --role-name my-eks-cluster-NodeGroupRole-oEOsIei9EnRD --policy-arn arn:aws:iam::aws:policy/service-role/AmazonEBSCSIDriverPolicy

himaniarr@GGL7HM2 MINGW64 ~/.kube
$  kubectl get pvc -n elk
NAME                                          STATUS    VOLUME   CAPACITY   ACCESS MODES   STORAGECLASS   VOLUMEATTRIBUTESCLASS   AGE
elasticsearch-master-elasticsearch-master-0   Pending                                                        <unset>                 7m59s
elasticsearch-master-elasticsearch-master-1   Pending                                                        <unset>                 7m59s
elasticsearch-master-elasticsearch-master-2   Pending                                                        <unset>                 7m59s

himaniarr@GGL7HM2 MINGW64 ~/.kube
$  kubectl describe pvc elasticsearch-master-elasticsearch-master-0 -n elk
Name:          elasticsearch-master-elasticsearch-master-0
Namespace:     elk
StorageClass:
Status:        Pending
Volume:
Labels:        app=elasticsearch-master
Annotations:   <none>
Finalizers:    [kubernetes.io/pvc-protection]
Capacity:
Access Modes:
VolumeMode:    Filesystem
Used By:       elasticsearch-master-0
Events:
  Type    Reason         Age                     From                         Message
  ----    ------         ----                    ----                         -------
  Normal  FailedBinding  2m24s (x26 over 8m38s)  persistentvolume-controller  no persistent volumes available for this claim and no storage class is set

himaniarr@GGL7HM2 MINGW64 ~/.kube
$ vim storage-class.yaml

himaniarr@GGL7HM2 MINGW64 ~/.kube
$ kubectl apply -f storage-class.yaml
storageclass.storage.k8s.io/aws-ebs created

himaniarr@GGL7HM2 MINGW64 ~/.kube
$  kubectl describe pvc elasticsearch-master-elasticsearch-master-0 -n elk
Name:          elasticsearch-master-elasticsearch-master-0
Namespace:     elk
StorageClass:
Status:        Pending
Volume:
Labels:        app=elasticsearch-master
Annotations:   <none>
Finalizers:    [kubernetes.io/pvc-protection]
Capacity:
Access Modes:
VolumeMode:    Filesystem
Used By:       elasticsearch-master-0
Events:
  Type    Reason         Age                From                         Message
  ----    ------         ----               ----                         -------
  Normal  FailedBinding  58s (x42 over 11m)  persistentvolume-controller  no persistent volumes available for this claim and no storage class is set
```

```
himaniarr@GGL7HM2 MINGW64 ~/.kube
$ kubectl apply -f storage-class.yaml
The StorageClass "gp2" is invalid:
* provisioner: Forbidden: updates to provisioner are forbidden.
* volumeBindingMode: Invalid value: "Immediate": field is immutable

himaniarr@GGL7HM2 MINGW64 ~/.kube
$ vim storage-class.yaml

himaniarr@GGL7HM2 MINGW64 ~/.kube
$ vim storage-class.yaml

himaniarr@GGL7HM2 MINGW64 ~/.kube
$ kubectl get storageclass
NAME      PROVISIONER             RECLAIMPOLICY   VOLUMEBINDINGMODE      ALLOWVOLUMEEXPANSION   AGE
aws-ebs   ebs.csi.aws.com         Delete          Immediate              false                  3m54s
gp2       kubernetes.io/aws-ebs   Delete          WaitForFirstConsumer   false                  27m

himaniarr@GGL7HM2 MINGW64 ~/.kube
$ kubectl get pvc
No resources found in default namespace.

himaniarr@GGL7HM2 MINGW64 ~/.kube
$ kubectl get pvc -n=elk
NAME                                          STATUS    VOLUME   CAPACITY   ACCESS MODES   STORAGECLASS   VOLUMEATTRIBUTESCLASS   AGE
elasticsearch-master-elasticsearch-master-0   Pending                                                        <unset>                 21m
elasticsearch-master-elasticsearch-master-1   Pending                                                        <unset>                 21m
elasticsearch-master-elasticsearch-master-2   Pending                                                        <unset>                 21m

himaniarr@GGL7HM2 MINGW64 ~/.kube
$ kubectl patch pvc elasticsearch-master-elasticsearch-master-0 -n elk -p '{"spec":{"storageClassName":"gp2"}}'
persistentvolumeclaim/elasticsearch-master-elasticsearch-master-0 patched

himaniarr@GGL7HM2 MINGW64 ~/.kube
$ kubectl get pvc -n=elk
NAME                                          STATUS    VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS   VOLUMEATTRIBUTESCLASS   AGE
elasticsearch-master-elasticsearch-master-0   Bound     pvc-387ca356-5d52-45f3-a90e-35919a2c7b5a   30Gi       RWO            gp2            <unset>                 21m
elasticsearch-master-elasticsearch-master-1   Pending                                                                                   <unset>                 21m
elasticsearch-master-elasticsearch-master-2   Pending                                                                                   <unset>                 21m
```

```
himaniaro@GGL7HM2 MINGW64 ~/.kube
$ kubectl patch pvc elasticsearch-master-elasticsearch-master-1 -n elk -p '{"spec":{"storageClassName":"gp2"}}'
persistentvolumeclaim/elasticsearch-master-elasticsearch-master-1 patched

himaniaro@GGL7HM2 MINGW64 ~/.kube
$ kubectl patch pvc elasticsearch-master-elasticsearch-master-2 -n elk -p '{"spec":{"storageClassName":"gp2"}}'
persistentvolumeclaim/elasticsearch-master-elasticsearch-master-2 patched

himaniaro@GGL7HM2 MINGW64 ~/.kube
$ kubectl get pods -n=elk
NAME                     READY   STATUS    RESTARTS   AGE
elasticsearch-master-0   0/1     Running   0          23m
elasticsearch-master-1   0/1     Running   0          23m
elasticsearch-master-2   0/1     Running   0          23m

himaniaro@GGL7HM2 MINGW64 ~/.kube
$  helm install logstash elastic/logstash --namespace elk
NAME: logstash
LAST DEPLOYED: Thu Jun 20 02:37:43 2024
NAMESPACE: elk
STATUS: deployed
REVISION: 1
TEST SUITE: None
NOTES:
1. Watch all cluster members come up.
  $ kubectl get pods --namespace=elk -l app=logstash-logstash -w

himaniaro@GGL7HM2 MINGW64 ~/.kube
$ kubectl get pods -n elk
NAME                     READY   STATUS    RESTARTS   AGE
elasticsearch-master-0   1/1     Running   0          25m
elasticsearch-master-1   1/1     Running   0          25m
elasticsearch-master-2   1/1     Running   0          25m
logstash-logstash-0      0/1     Running   0          26s

himaniaro@GGL7HM2 MINGW64 ~/.kube
$  helm install kibana elastic/kibana --namespace elk
NAME: kibana
LAST DEPLOYED: Thu Jun 20 02:38:59 2024
NAMESPACE: elk
STATUS: deployed
REVISION: 1
TEST SUITE: None
NOTES:
1. Watch all containers come up.
  $ kubectl get pods --namespace=elk -l release=kibana -w
2. Retrieve the elastic user's password.
  $ kubectl get secrets --namespace=elk elasticsearch-master-credentials -ojsonpath='{.data.password}' | base64 -d
3. Retrieve the kibana service account token.
  $ kubectl get secrets --namespace=elk kibana-kibana-es-token -ojsonpath='{.data.token}' | base64 -d
```

```
himaniaro@GGL7HM2 MINGW64 ~/.kube
$ kubectl get pods -n elk
NAME                            READY   STATUS    RESTARTS   AGE
elasticsearch-master-0          1/1     Running   0          35m
elasticsearch-master-1          1/1     Running   0          35m
elasticsearch-master-2          1/1     Running   0          35m
kibana-kibana-555ddb75f-c6768   1/1     Running   0          7m59s
logstash-logstash-0             1/1     Running   0          9m51s

himaniaro@GGL7HM2 MINGW64 ~/.kube
$ kubectl get secret elasticsearch-master-credentials -n elk -o yaml
apiVersion: v1
data:
  password: VEhLaldYQ2Z6TDEwUXAyNQ==
  username: ZWxhc3RpYw==
kind: Secret
metadata:
  annotations:
    meta.helm.sh/release-name: elasticsearch
    meta.helm.sh/release-namespace: elk
  creationTimestamp: "2024-06-19T20:42:33Z"
  labels:
    app: elasticsearch-master
    app.kubernetes.io/managed-by: Helm
    chart: elasticsearch
    heritage: Helm
    release: elasticsearch
  name: elasticsearch-master-credentials
  namespace: elk
  resourceVersion: "2907"
  uid: e03e465b-c8cc-48d2-8da0-c9127fd40093
type: Opaque

himaniaro@GGL7HM2 MINGW64 ~/.kube
$ echo "ZWxhc3RpYw=="| base64 --decode
elastic
himaniaro@GGL7HM2 MINGW64 ~/.kube
$ echo "VEhLaldYQ2Z6TDEwUXAyNQ=="| base64 --decode
THKjWXCfzL10Qp25
himaniaro@GGL7HM2 MINGW64 ~/.kube
$ kubectl port-forward -n elk svc/kibana-kibana 5601:5601
Forwarding from 127.0.0.1:5601 -> 5601
Forwarding from [::1]:5601 -> 5601
Handling connection for 5601
Handling connection for 5601
Handling connection for 5601
```


elastic
Find apps, content, and more.
Discover
apache1
Options
New
Open
Share
Alerts
Inspect
Save
apache1
Filter your data using KQL syntax
May 17, 2015 @ 15:35:00.000 → May 21, 2015 @ 02:35:59.000
Refresh
Search field names
Filter by type 0
_id
_index
_score
@timestamp
http.request.method
http.request.referrer
http.response.body.bytes
http.response.status_code
http.version
message
source.address
url.original
user_agent.original
9,986 hits
Reset search
200
100
0
12:00 18:00 May 17, 2015
00:00 May 18, 2015
06:00
12:00
18:00
00:00 May 19, 2015
06:00
12:00
18:00
00:00 May 20, 2015
06:00
12:00
18:00
00:00
May 17, 2015 @ 15:35:00.000 - May 21, 2015 @ 02:35:59.000 (interval: Auto - hour)
Documents
Field statistics
BETA
Get the best look at your search results
Add relevant fields, reorder and sort columns, resize rows, and more in the document table.
Take the tour
Dismiss
1 field sorted
@timestamp
Document
May 21, 2015 @ 02:35:59.000
@timestamp May 21, 2015 @ 02:35:59.000 http.request.method GET http.response.body.bytes 10,021 http.response.status_code 20
66.249.73.135 - - [20/May/2015:21:05:59 +0000] "GET /blog/tags/wine HTTP/1.1" 200 10021 "-" "Mozilla/5.0 (iPhone; CPU iPhone
source.address 66.249.73.135 url.original /blog/tags/wine user_agent.original Mozilla/5.0 (iPhone; CPU iPhone OS 6_0 like
May 21, 2015 @ 02:35:59.000
@timestamp May 21, 2015 @ 02:35:59.000 http.request.method GET http.response.body.bytes 3,894 http.response.status_code 200