How to make the best use of Live Sessions

- Please login on time
- Please do a check on your network connection and audio before the class to have a smooth session
- All participants will be on mute, by default. You will be unmuted when requested or as needed
- Please use the “Questions” panel on your webinar tool to interact with the instructor at any point during the class
- Ask and answer questions to make your learning interactive
- Please have the support phone number (US : 1855 818 0063 (toll free), India : +91 90191 17772) and raise tickets from LMS in case of any issues with the tool
- Most often logging off or rejoining will help solve the tool related issues

COURSE OUTLINE

Module 06

Introduction to Kubernetes

Kubernetes Architecture

Deploy app to Kubernetes Cluster

Expose App, Scale App And Update App

Managing State with Deployments

Federations, Auditing and Debugging Kubernetes, Security best practices

edureka!

Federations, Auditing and Debugging Kubernetes, Security Best Practices

Objectives

After completing this module, you should be able to understand:

- Federated clusters
- Debugging by looking at the events
  - Pending Pods
  - Unreachable nodes
- Auditing and accessing logs in Kubernetes – Log collectors and audit policy
- Security best practices in Kubernetes

Federated clusters

edureka!

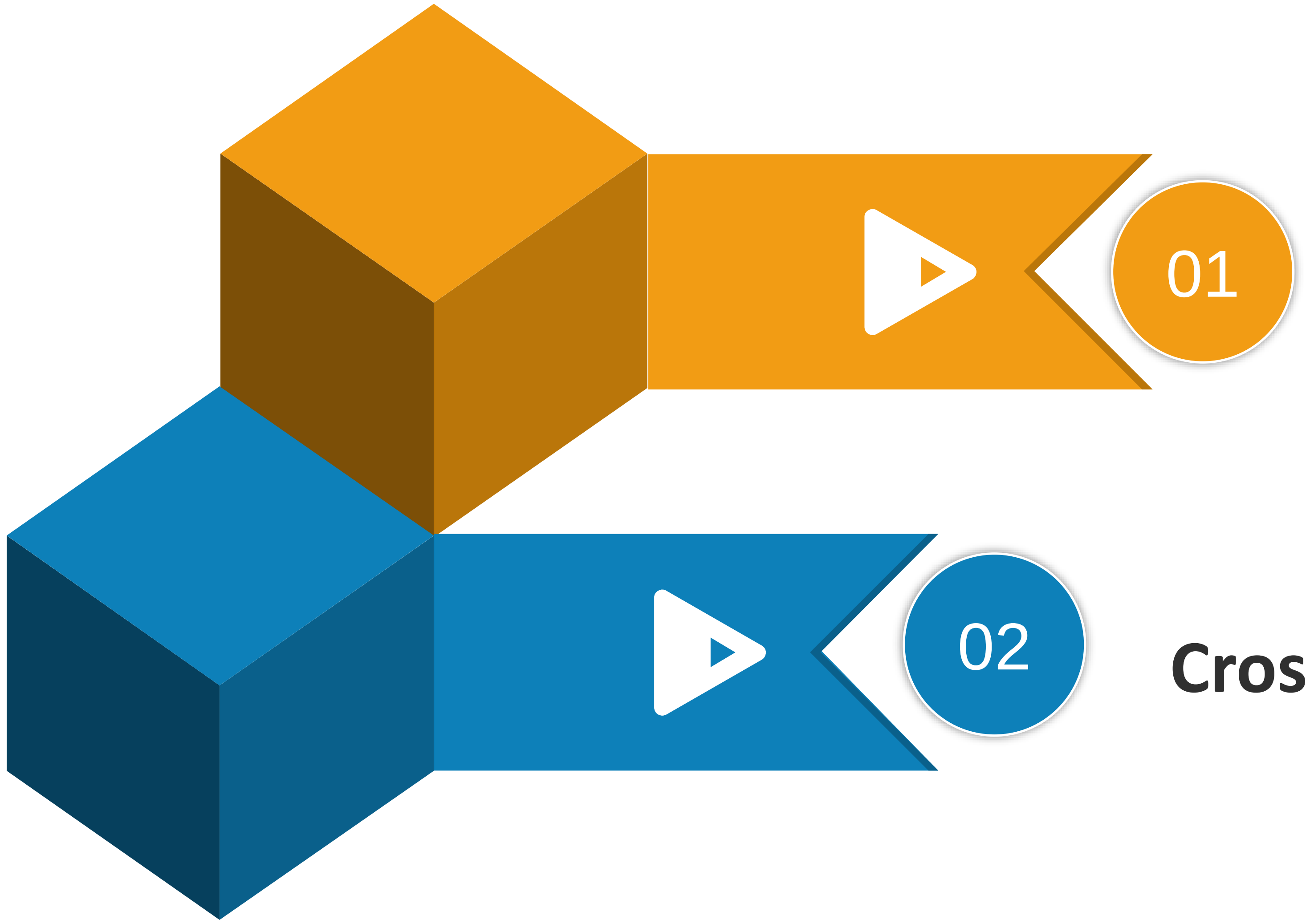
Federated Clusters

Cluster Federation

It is something using which you can manage multiple Kubernetes clusters as if they were one.)

- In other words, you have the freedom to create multiple kubernetes cluster within your datacenter or in cloud and use federation to control / manage them all at one place.
- And it is able to achieve this by doing two things :
    - Sync resources across clusters
    - Cross cluster discovery

Federated Clusters



Sync resources across clusters

- As the name suggest, Federation help to keep the resource sync across multiple cluster.
- Consider, same deployment set exist across multiple cluster.

Cross cluster discovery

- It provides the ability to have DNS and Load Balancer with backend from all the participating cluster.
- Consider, having a DNS record to be used to access the multiple cluster.

Federated Clusters - Common Use-cases

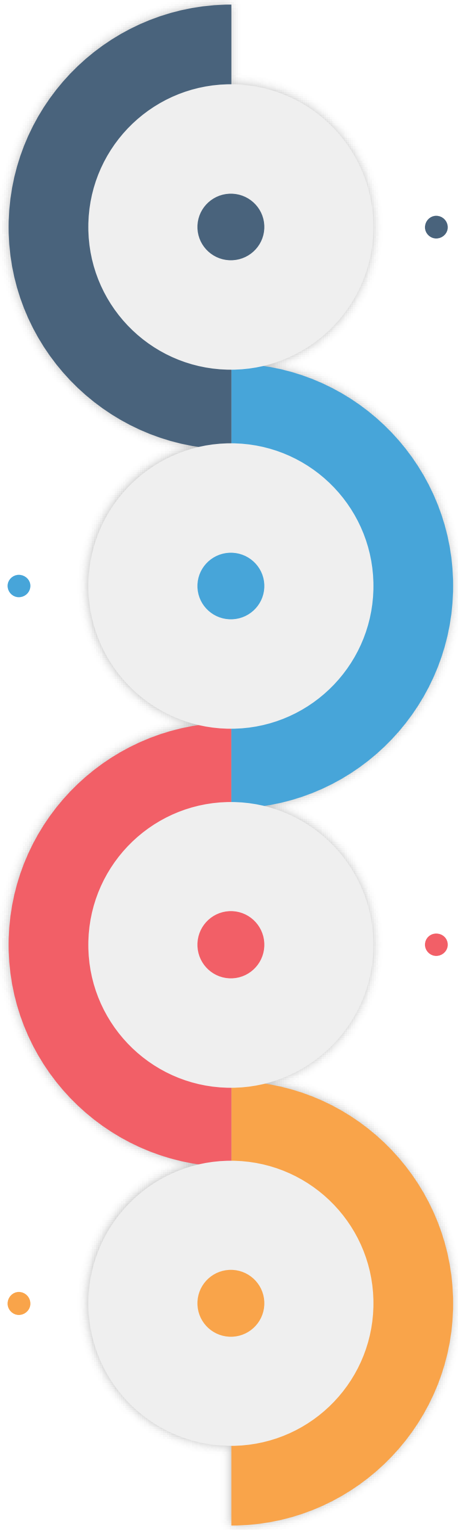
Provides better geographical coverage. It also helps in reducing the latency by serving the traffic closer to its geographical location as it provides flexibility to span across multiple cluster.

By leveraging the distribution of resources and having cross cluster discovery, it provides better reliability of the solution by minimizing the impact of cluster.

It also helps in creating hybrid-cluster by spreading resources across two cloud or mixing it with in-premise cluster.

It also provides flexibility to migrate workload from one cloud to another, this helps in removing any kind of dependency on cloud providers or vendors.

Federated Clusters - Cons



It is a costly solution, as it consumes more resources and also keep the resource in sync.

This leads to higher cost.

Since multiple clusters are in sync, it increases the higher risk of security breach.

Also, if there is one bug then it may impact the whole cluster.

Debugging

Debugging by looking at the events

- Kubernetes events are APi objects which provides visibility inside the cluster to understand what exactly is happening.
- This helps in debugging the cluster and also applications by providing insight, like how scheduler is behaving or what led other Pods terminate etc.
- Since events are API objects, they are stored in the apiserver on master.
- There are few precautions are taken in which prevents event from filling out the disk space.
- If longer event history needs to be preserved then one should use 3rd party solution.

☛ Stackdriver provides logging capabilities to events.

Debugging by looking at the events (Cont..)

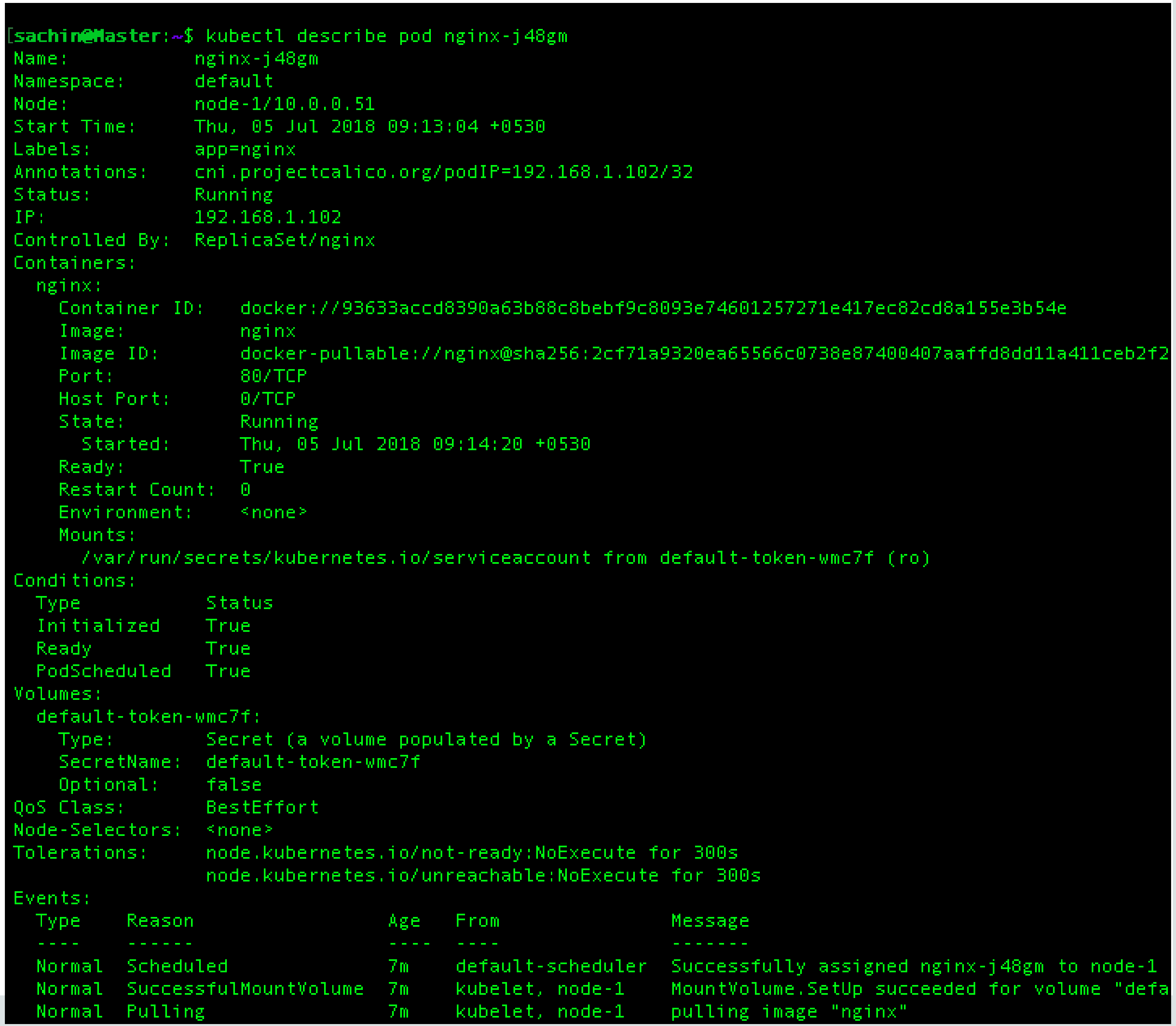
- Events in federation are similar to the events in traditional kubernetes events
- They both provide the same functionality.
- Events in federation are stored only at the federation control plan, they are not pushed to the backend kubernetes cluster.
- Federation controllers create events as they process API resources
- You can get all events from federation apiserver by running:

```
Kubectl --context=federation-cluster get events
```

Pod Pending status Reasons

- The very first thing which you need to do when Pod status is pending is –
  - Check the current state and events by following command:

```
$kubectl describe pods <pod_name>
```



```
[sachin@Master:~$ kubectl describe pod nginx-j48gm
Name:           nginx-j48gm
Namespace:      default
Node:           node-1/10.0.0.51
Start Time:     Thu, 05 Jul 2018 09:13:04 +0530
Labels:         app=nginx
Annotations:    cni.projectcalico.org/podIP=192.168.1.102/32
Status:         Running
IP:             192.168.1.102
Controlled By:  ReplicaSet/nginx
Containers:
  nginx:
    Container ID:   docker://93633accd8390a63b88c8bebf9c8093e74601257271e417ec82cd8a155e3b54e
    Image:          nginx
    Image ID:       docker-pullable://nginx@sha256:2cf71a9320ea65566c0738e87400407aaffd8dd11a411ceb2f2
    Port:           80/TCP
    Host Port:      0/TCP
    State:          Running
      Started:      Thu, 05 Jul 2018 09:14:20 +0530
    Ready:          True
    Restart Count:  0
    Environment:    <none>
    Mounts:
      /var/run/secrets/kubernetes.io/serviceaccount from default-token-wmc7f (ro)
Conditions:
  Type           Status
  Initialized    True
  Ready          True
  PodScheduled   True
Volumes:
  default-token-wmc7f:
    Type:        Secret (a volume populated by a Secret)
    SecretName:  default-token-wmc7f
    Optional:    false
QoS Class:       BestEffort
Node-Selectors:  <none>
Tolerations:     node.kubernetes.io/not-ready:NoExecute for 300s
                 node.kubernetes.io/unreachable:NoExecute for 300s
Events:
  Type    Reason                 Age   From               Message
  ----    ------                 ----  ----               -------
  Normal  Scheduled              7m    default-scheduler  Successfully assigned nginx-j48gm to node-1
  Normal  SuccessfulMountVolume  7m    kubelet, node-1    MountVolume.SetUp succeeded for volume "defa
  Normal  Pulling                7m    kubelet, node-1    pulling image "nginx"
```

edureka!

Pod Pending status Reasons (Cont..)

If status is ‘pending’ :

  - It happens when kubernetes Pod cannot be schedule on the available node.
  - In most of the cases, it is been seen that it happens mainly because of resource shortage.
  - ‘Kubectl describe.. Command gives the details about the root cause.
- To fix this, add more resource to the cluster
- Add more nodes
- Set resource quota
- Remove not-required Pods

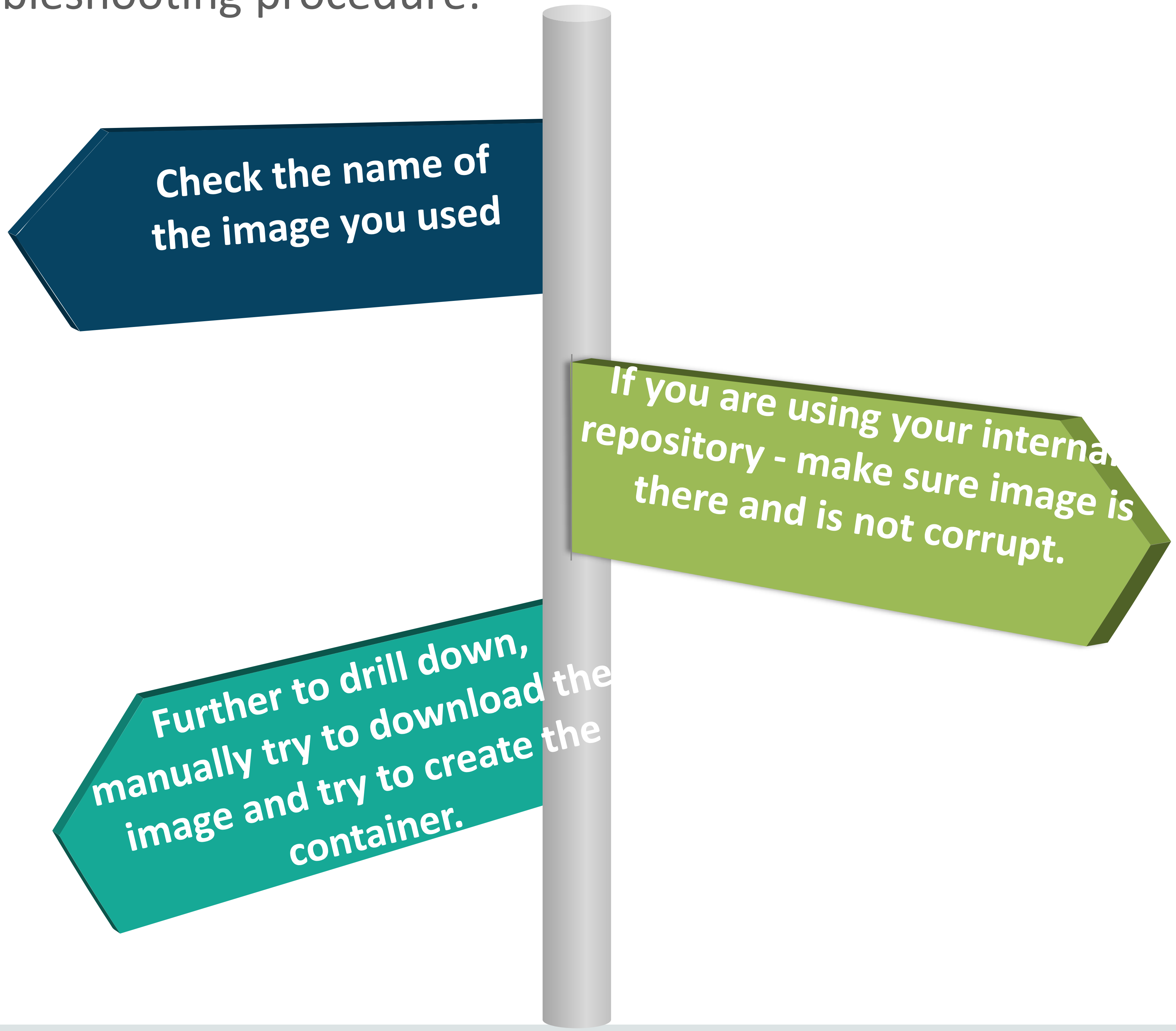
Pod Pending status Reasons (Cont..)

If status is ‘waiting’ :

- It means that it has been scheduled to a worker node, but it cannot run on that machine.
- Again, follow the same approach and use ‘kubectl describe <pod_name> to get more details about the Pod.
- Eg. One of the cause is - pod is not able to pull the image from the repository.

Troubleshooting

- Now the traditional troubleshooting procedure:



Check the name of the image you used

If you are using your internal repository - make sure image is there and is not corrupt.

Further to drill down, manually try to download the image and try to create the container.

Pod Pending status Reasons (Cont..)

Pod is unhealthy or crashing:

- In this also, you need to follow the traditional troubleshooting approach
- Use

```
kubectl describe pod <pod_name>
Kubectl logs <pod_name>
```

  - ‘Also see the system logs.
  - Also check the kubectl version
  - Rediirect the log file : terminationMessagePath: “/tmp/log”

Unreachable nodes

If node is unreachable :

- Kubernetes version 1.5v or newer will not delete Pods instead it will do following:
- Put Pod into ‘Terminating’ or ‘Unknown’ status after the timeout.

This might also happen if user tries to delete the Pod on an unrechable node.

- In such scenarios, the only ways in which a Pod can be removed from the apiserver are as follows:
- The Node object is deleted.
- kubelet on the unresponsive Node starts responding, kills the Pod and removes the entry from the apiserver.
- Force deletion of the Pod by the user.

Unreachable nodes (Cont..)

- Kubernetes nodes are treated as cattle.
- Main objective should be that all the Pods which are serving application gets created on another Pod which is reachable and working fine.
- 1, 2 or couple of other nodes going down in the kubernetes cluster will not cause any major impact
- If any node goes down, make sure all the pods are created on other available nodes and work to fix the problem with the faulty node.

Auditing and accessing logs in Kubernetes

Auditing and accessing logs in Kubernetes

- Just like any other auditing, Kubernetes auditing also targets to capture sequence of events which has affected the system.
- Auditing could be done by :
  - end user,
  - administrator or
  - some components within the system.
- Objected is to find as much information as possible (like what happened, when did it happen, who did it, under what conditions it happened, etc)what happened?

Auditing and accessing logs in Kubernetes (Cont..)

Kube-apiserver

- Auditing is done by the kube-apiserver.
    - Every request at different stages generates an event.
    - This event gets processed by policies and once it is processed, it gets written to a backend.
    - Policy determine what gets recorded in the backend, which determines to hold the records.
    - Each request is associated with a stage.

Request Stages

Each request is associated with a stage.

Panic
It notifies and creates a event

RequestReceived
Notifies that audit handler has received the request.

ResponseComplete:
Once all the Response are sent. No further data will be sent for the particular event.

ResponseStarted
For long running request, Response header are sent before the response body is sent.

edureka!

Audit Policy

Audit Policy

Audit policy defines what data should be included from the event and what should be recorded

- At the time of event processing, it gets compared against the rules defined under policy in chronological order.
- First matching rule sets the ‘audit level’ for the event.
  - There are four stages as explanined in next slide.

Stages of audit level

None
Don’t log any event which matches this module.

RequestResponse
log metadata, request and response bodies of events.
This does not apply for non-resource requests

Metadata means :
Requesting user,
Timestamp,
Resource,
Verb, etc

Metadata:
Log metadata only. Don’t log the request and event body.

Request
log metadata and request. Don’t log the event body.
This does not apply for non-resource requests

Audit Backend

Audit Backend: Audit backends persist audit events to an external storage.

There are two backend provided by Kube-api server:

Log backend

Webhook backend

- **Log backend** - writes events to a disk
- **Webhook backend** this sends events to an external API and later it gets written to external storage.

Log Collector

- If you are having multi-cluster scenario then you can configure aggregation layer to extend your kubernetes API, and setup audit logging for the aggregated apiserver.
- The aggregation layer enables installing additional Kubernetes-style APIs in your cluster
- Different apiservers can have different audit configurations and different audit policies
- For log collector: You can use ‘fluentd’ to collect and distribute audit events from log file.

Fluentd

As per the official definition from website : https://www.fluentd.org/

"

Fluentd is an open source data collector for unified logging layer."

Fluentd

Open source data collector for unified logging layer

- For better understanding and usage of data, it allows to unify data collection and consumption
- Fluentd provides a unified logging layer between data source and backend systems.
- This helps to decouple data source from backend systems.

Logstash

- Logstash:
  - ‘ https://www.elastic.co/products/logstash ‘
- There is another ‘Legacy audit’ but it is not deprecated and will be removed completely from v1.12.

Logstash

It is another opensource tool for data processing.
It is a server-side data processing tool that takes data from multiple sources simultaneously.

Security best practices in Kubernetes

Security best practices in Kubernetes

- Running containers without security opens up high risk of getting compromised.
- Kubernetes provides multiple options for securing the Pods. And configuring them with proper policies and security standards help in achieving the required security for the kubernetes cluster environment.
- There are few guidelines provided by kubernetes which ensures that maximum security can be attained for the workload you are running on the cluster.

Security best practices in Kubernetes (Cont..)

If we can ensure there are no software components with known vulnerabilities, many of the security threats can be mitigated.

To ensure this:

Implement Continuous Security Vulnerability Scanning

- After the initial deployment of the containers, it is important to apply the relevant security patches. There are multiple security patches are released almost everyday and it is very important and it is very important to have a process in place, where images are continuously assessed and applied accordingly.

Regularly Apply Security Updates to Your Environment

- Avoid updating / applying patches directly from upstream. Instead use Kubernetes rolling updates feature to apply the required patches.

edureka!

Security best practices in Kubernetes (Cont..)

Couple of other best practices are :

Provide limited direct access to kubernetes nodes :

- Use "kubectl exec" to provide direct access to the container environment instead of direct access through SSH.

Define strict policy / rules for resources:

- Limiting the scope of user permissions can reduce the impact of mistakes or malicious activities. However, kubernetes namespace allows creating resources into logically named groups and there it's becomes important for you to put proper policy for users to access the resources.

edureka!

Security best practices in Kubernetes (Cont..)

Use Images from authorized repository only

- Make sure images which you are using are adhered to organization’s policy .
- Downloading and running images from unknown sources is dangerous.
- Create your own local repository of tested and trusted images to be used in production environment.

Define Resource Quota

- Not defining resources properly and not putting limitation, increases the risk of having “noisy neighbor” or ‘DoS’ attacks.

Security best practices in Kubernetes (Cont..)

Implement Network Segmentation

- Network segmentation is important to ensure that containers can communicate only with those they are supposed to. It also restrict the spread of attack from one network to other.

Log everything on Production environment

- You can only fix the gaps, bugs which you are aware of . And this is where it becomes very important for you keep track of all the activities happening in your environment.

Security best practices in Kubernetes (Cont..)

Enable auditing

- Though it is beta release but it is one of the important feature to have proper security in the cluster.
- This gives you the capability to do the analysis at later stage.

Restrict access to etcd:

- It holds all the important metadata about the environment and it is very important to secure this.

Quiz

1. What do you understand by **Cluster Federation?**

Answers

1. What do you understand by Cluster Federation?

Answer : It is something using which you can manage multiple Kubernetes clusters as if they were one.

Quiz

2. Cross cluster discovery: It provides the ability to have DNS and Load Balancer with backend from all the participating cluster.

    a. True

    b. False

Answers

2. Cross cluster discovery: It provides the ability to have DNS and Load Balancer with backend from all the participating cluster.

   a. [✓ True]

   b. False

Answer A: True

Quiz

3. Give any 2 use-cases of cloud federation.

Answers

3. Give any 2 use-cases of cloud federation.

Answer C:

1. By leveraging the distribution of resources and having cross cluster discovery, it provides better reliability of the solution by minimizing the impact of cluster.

2. It also provides flexibility to migrate workload from one cloud to another, this helps in removing any kind of dependency on cloud providers or vendors.

Quiz

4. Following are the benefits of cloud federation

- It is a costly solution, as it consumes more resources and also keep the resource in sync.
- This leads to higher cost.
- Since multiple clusters are in sync, it increases the higher risk of security breach.

a. True

b. False

Answers

4. Following are the benefits of cloud federation

- It is a costly solution, as it consumes more resources and also keep the resource in sync.
- This leads to higher cost.
- Since multiple clusters are in sync, it increases the higher risk of security breach.

   a. True

   b. [✓ False]

Answer B: False

Quiz

5. Match the following for different stages of auditing:

1. RequestReceived a: Notifies that audit handler has received the request.

2. ResponseStarted b: For long running request, Response header are sent before the response body is sent.

3. ResponseComplete c: Once all the Response are sent. No further data will be sent for the particular event.

Answers

5. Match the following for different stages of auditing:

1. RequestReceived a: Notifies that audit handler has received the request.

2. ResponseStarted b: For long running request, Response header are sent before the response body is sent.

3. ResponseComplete c: Once all the Response are sent. No further data will be sent for the particular event.

Answer :
1: a
2: b
3: c

Quiz

6. Fill in the blanks

   a. Log backed writes ………

   b. Webhooks backend sends …..

Answers

6. Fill in the blanks

   a. Log backed writes ………

   b. Webhooks backend sends …..

Answer :

Log backend - writes events to a disk

Webhook backend this sends events to an external API and later it gets written to external storage.

Quiz

7. What is log-collector ?

Answers

7. What is log-collector ?

Answer :
The aggregation layer enables installing additional Kubernetes-style APIs in your cluster

Quiz

8. What is fleuntd?

Answers

8. What is fleuntd?

Answer :

Fluentd is an open source data collector for unified logging layer.

Fluentd allows you to unify data collection and consumption for a better use and understanding of data.

Quiz

9. Logstash is a server-side data processing tool that takes data from multiple sources simultaneously.

   a. True

   b. False

Answers

9. Logstash is a server-side data processing tool that takes data from multiple sources simultaneously.

   a.

   b. False

Answer A: True

Quiz

10. Give any 3 best practises for securing your kubernetes cluster

Answers

10. Give any 3 best practises for securing your kubernetes cluster

Answer :
Enable auditing
Restrict access to etcd
Implement Network Segmentation

We have discussed about 8 of them. Choose any 3 from it.

Summary

- In this module, you should have learnt:
- Federated clusters
- Debugging by looking at the events
  - Pending Pods
  - Unreachable nodes
- Auditing and accessing logs in Kubernetes – Log collectors and audit policy
- Security best practices in Kubernetes

edureka!

Questions

edureka!

OPINION
SURVEY
RESPONSE
COMMENT
FEEDBACK
IDEA
ADVICE
RESULT
RATING

edureka!

Thank You

For more information please visit our website
www.edureka.co