Certified Kubernetes Administrator Prep

Securing Cluster Communications

Cluster Communications

- Cluster communications cover communication to the API server, control-plane communications inside the cluster, and can even include pod-to-pod communications.

- This is an in-depth topic with a fair amount of detail, so let's start by discussing how to secure communications to the Kubernetes API server.

- Everything in Kubernetes goes through the API driver, so controlling and limiting who has access to the cluster and what they are allowed to do is arguably the most important task in securing the cluster.

Cluster Communications

- The default encryption communication in K8s is TLS
- Most of the installation methods will handle the certificate creation
- Kubeadm created certificates during the Linux Academy Cloud Server Kubernetes Cluster lab.
- No matter how you've install kubernetes, some components and installation methods may enable local ports over HTTP and you should double check the settings of these components to identify potentially unsecured traffic and address these issues.

Cluster Communications

- Anything that connects to the API, including nodes, proxies, the scheduler, volume plugins in addition to users, should be authenticated.
- Again, most installation methods create certificates for those infrastructure pieces, but if you’ve chosen to install manually, you might need to do this yourself.
- Once authenticated, every API call should pass an authorization check.

Role-Based Access Control

- Kubernetes has an integrated Role-Based Access Control (RBAC) component
- Certain roles perform specific actions in the cluster
- Kubernetes has several well thought out, pre-created roles

Role-Based Access Control

- Simple roles might be fine for smaller clusters
- If a user doesn’t have rights to perform an action but they do have access to perform a composite action that includes it, the user WILL be able to indirectly create objects.
- Carefully consider what you want users to be allowed to do prior to making changes to the existing roles.

Securing the Kubelet

- Secure the kubelet on each node.
- The Kubelets expose HTTPS endpoints which give access to both data and actions on the nodes. By default, these are open.
- To secure those endpoints, you can enable Kubelet Authentication and Authorization by starting it with an --anonymous-auth=false flag and assigning it an appropriate x509 client certificate in its configuration.

Securing the Network

- Network Policies restrict access to the network for a particular namespace.

- This allows developers to restrict which pods in other namespaces can access pods and ports within the current namespace.

- The pod networking CNI must respect these policies which, fortunately, most of them do.

Securing the Network

Users can also be assigned quotas or limit ranges

Use Plug-Ins for more advanced functionality

That should secure all the communications in a cluster

Vulnerabilities

- Kubernetes makes extensive use of etcd for storing configuration and secrets. It acts as the key/value store for the entire cluster.
- Gaining write access to etcd is very much like gaining root on the whole cluster, and even read access can be used by attackers to cause some serious damage.
- Strong credentials on your etc server or cluster is a must.
- Isolate those behind a firewall that only allows requests from the API servers

Vulnerabilities

- Audit logging is also critical
- Records actions taken by the API for later analysis in the event
- Enable audit logging and archive the audit file on a secure server

Vulnerabilities

- Rotate your infrastructure credentials frequently
- Smaller lifetime windows for secrets and credentials create bigger problems for attackers attempting to use it.
- You can even set these up to have short lifetimes and automate their rotation.

Third Party Integrations

- Always review third party integrations before enabling them.
- Integrations to Kubernetes can change how secure your cluster is.
- Add-ons might be nothing more than just more pods in the cluster, but those can be powerful.
- Don’t allow them into the kube-system namespace.

Conclusion

- You should also join the kubernetes-announce group for emails about security announcements.
    - (url -> https://groups.google.com/forum/#!forum/kubernetes-announce)

- In this lesson we've discussed:
    - How to secure communications in your kubernetes cluster including the api server.
    - The individual kubelets on the nodes, and your etc server.
    - Networking policies and providers.
    - Some tips on keeping your cluster safe and secure.