**Security**

## **Security Primitives**

**Secure Host**

A picture containing text

Description automatically generated

All access to these hosts must be secured, root access disabled, password based authentication disabled and only SSH key based authentication to be made available.

**Secure Kubernetes**

Graphical user interface, text, chat or text message

Description automatically generated

Who can access the API server is defined by the Authentication mechanism. There are dif ways to authenticate to the API server.

Text

Description automatically generated

Text

Description automatically generated

All communication with the cluster between the various components such as the ETCD cluster, kube controller manager, scheduler, api server as well as those running on the worker node such as kubelet and kubeproxy is secured using **TLS Encryption.**

Diagram

Description automatically generated

By Default all the pods can access all other PODs within the cluster. It can be restricted using Network policies.

Chart, diagram, schematic, bubble chart

Description automatically generated

## **Authentication**

Graphical user interface

Description automatically generated

K8 is not managing user accounts natively , it relies on external sources file with user details, certificates, or like LDAP.

K8 can able to manage the service accounts.

All the user access are managed by the API server. Whether you are access it thr kubectl or directly to the API server. All of the request go the kube API server . Then Kube APi server Authenticates the request before processing it.

A picture containing diagram

Description automatically generated

**How does it Authenticate ??**

* Static Password file
* Static Token File
* Certificates
* Identity Service

**Static Password file**

Graphical user interface, text

Description automatically generated

Password in csv file. The file has three column password username & userid.

You can pass the file as parameter or configure inside the apiserver.service file.

**--basic-auth-file=user-details.csv**

Text

Description automatically generated

To authenticate using the basic cred while accessing the API server, specify the user and password in curl command.

Text

Description automatically generated

A screenshot of a computer

Description automatically generated with medium confidence

In csv file we can optionall add fourth column for group.

## **TLS Basics**