In a distributed model, such as the one used by Docker Swarm, it is important to encrypt communication between nodes to prevent potential attackers from obtaining sensitive data from network communications. In this lesson, we'll discuss the two ways that Docker Swarm utilizes for securing cluster communication. We'll also cover how to encrypt overlay network communication to secure the communication between containers within the cluster, and we'll discuss how Docker Swarm uses Mutually Authenticated Transport Layer Security (MTLS) to encrypt and authenticate cluster-level communication.

Relevant Documentation

- https://docs.docker.com/engine/swarm/how-swarm-mode-works/pki/
- https://docs.docker.com/v17.09/engine/userguide/networking/overlay-security-model/

Lesson Reference

Create an encrypted overlay network:

```
docker network create --opt encrypted --driver overlay my-encrypted-net
```

Create two services on the encrypted overlay network and demonstrate that one service can communicate with the other:

```
docker service create --name encrypted-overlay-nginx --network my-encrypted-net --replicas 3 nginx
docker service create --name encrypted-overlay-busybox --network my-encrypted-net radial/busyboxplus:curl sh
```

Check the logs for the `busybox` service, and then verify that it shows the Nginx welcome page:

```
docker service logs encrypted-overlay-busybox
```