Introduction

Pod network corruption in chaos engineering refers to intentionally causing disruptions or failures in the networking layer of Kubernetes pods to test the resilience of the system.

In a Kubernetes cluster, pods communicate with each other over the network, and any disruption in this communication can lead to service outages or degraded performance. By simulating network corruption, such as introducing packet loss, delays, or dropping network packets, chaos engineers can evaluate how well their system handles such failures.

The goal of chaos engineering is to identify weaknesses in the system's design or configuration before they cause problems in production. By deliberately inducing failures and observing how the system responds, engineers can improve its resilience and ensure better overall reliability.

* It injects packet corruption on the specified container by starting a traffic control (tc) process with netem rules to add egress packet corruption.
* It can test the application's resilience to lossy/flaky network.

Impact

The impact of Pod Network Duplication chaos attack can be seen using: **ping <pod-ip> , through another cluster pod** command in the desired namespace.