@awsgeek | AWS 2017 RE:INVENT | CONTAINER NETWORKING DEEP DIVE WITH ECS | CON401 | jerry.hargrove

CLUSTER

LOGICAL INFRA ISOLATION
IAM PERMISSION BOUNDARY

EC2 INSTANCES

SERVICE

- MAINTAIN RUNNING TASKS
- INTEGRATED WITH ALB
- REPLACE UNHEALTHY TASKS

TASK

CONTAINER CONFIG

IMAGE, CPU, NETWORKING, PORTS, RAM, etc

CONTAINER

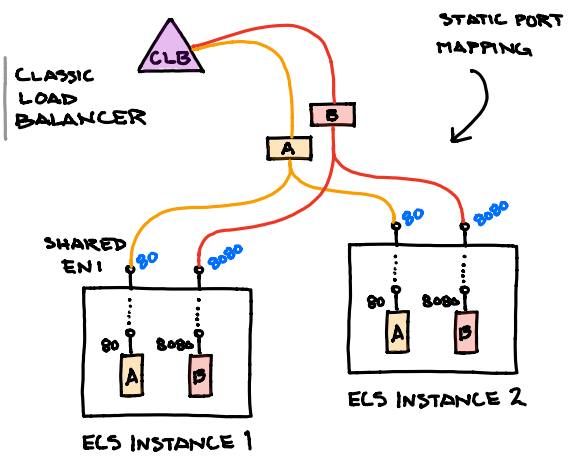
CODE AND DEPENDENCIES

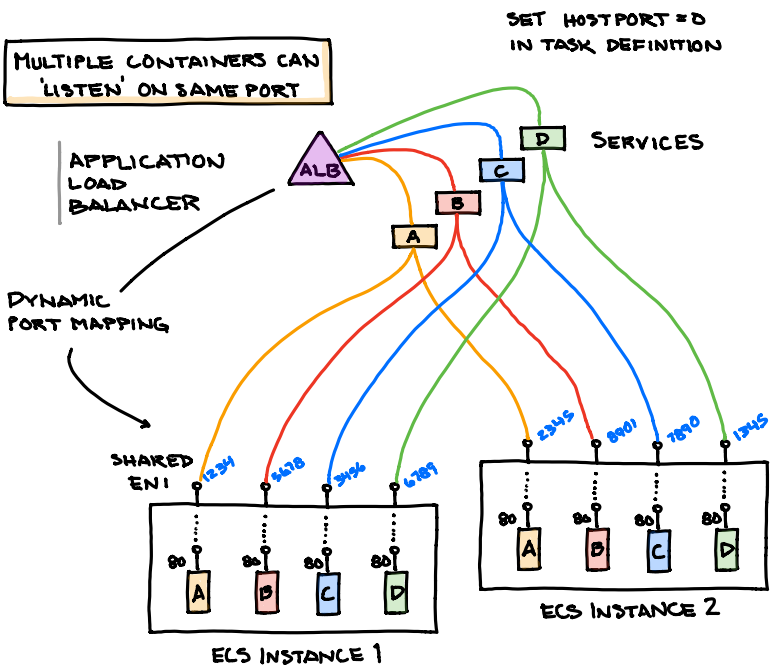
ELASTIC NETWORK INTERFACE (ENI)

- 1 PRIMARY PRIVATE IPV4
- 1+ SECONDARY PRIVATE IPV4
- 1 PUBLIC IPV4
- 1+ IPV6
- 1+ SECURITY GROUPS
- MAC ADDRESS

CLOUD NATIVE COMPUTING FOUNDATION

CONTAINER NETWORKING INTERFACE

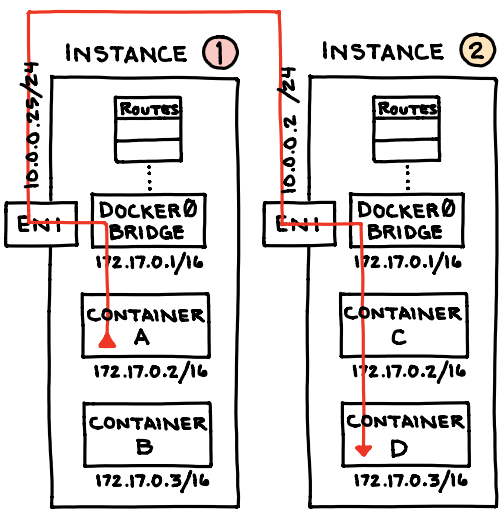




NETWORK MODES

BRIDGE MODE

- SINGLE ENI PER INSTANCE
- ALL TASKS SHARE SAME ENI
- ALL EXTERNAL TRAFFIC ROUTED THRU DOCKER0 BRIDGE
- FINE GRAINED SECURITY IS DIFFICULT
- TASKS ARE UNROUTABLE



NEW TASK (AWSVPC) MODE

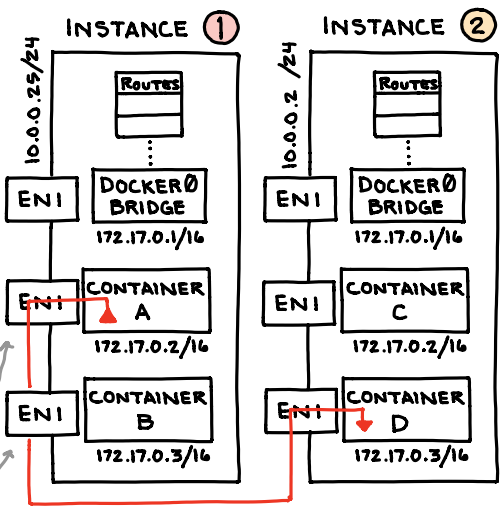
GOAL: MAKE TASKS 1ST CLASS NETWORKING CONSTRUCT

- ENI CREATED ON YOUR BEHALF, ASSIGNED TO TASK
- ENI GIVEN PRIVATE IP FROM USER SPECIFIED SUBNET
- DEFAULT SECURITY GROUP ALLOWS LOCAL TRAFFIC ONLY
- ALLOWS FINE-GRAINED SECURITY
- TASKS ARE ROUTABLE

ENI LIMITS PER EC2 INSTANCE TYPE STILL APPLY

TO AVOID ENI LIMITS, USE FARGATE

CNI PLUGIN CONFIGURES EACH TASK ENI



PACKET PATH BETWEEN TASK A & TASK D