Building Serverless with K8S, Kata Containers and Bare Metal Cloud In Alibaba

Yifei Zhang     Senior Enigneer in Alibaba Cloud
Huamin Tang     Engineer II in Alibaba Cloud
Outline

• Serverless Overview

• Serverless Platform Construction

• Kata Containers

• Q&A
Serverless Overview – Status Quo

- Maintenance
- Best Practices
- Effective Iteration
- Quick Response
Serverless Overview – Problem Domains

- Reduce the Cost of Operation and Maintenance
- Reduce the Cost of Development
Serverless Overview – Definition

Wikipedia:

- Serverless computing is a cloud-computing execution model in which the cloud provider runs the server, and dynamically manages the allocation of machine resources. Pricing is based on the actual amount of resources consumed by an application, rather than on pre-purchased units of capacity.

- Serverless computing can simplify the process of deploying code into production. Scaling, capacity planning and maintenance operations may be hidden from the developer or operator. Serverless code can be used in conjunction with code deployed in traditional styles, such as microservices. Alternatively, applications can be written to be purely serverless and use no provisioned servers at all.
## Serverless Overview – Roles

<table>
<thead>
<tr>
<th>User</th>
<th>Platform</th>
</tr>
</thead>
<tbody>
<tr>
<td>- No need to care about the server</td>
<td>- Provide resource pool services</td>
</tr>
<tr>
<td>- Pay by usage</td>
<td>- Provide on-demand metering and billing services</td>
</tr>
<tr>
<td>- Auto scaling</td>
<td>- Provide auto-scaling services</td>
</tr>
<tr>
<td>- etc.</td>
<td>- Provide secure data surface services</td>
</tr>
<tr>
<td></td>
<td>- etc.</td>
</tr>
</tbody>
</table>
Serverless Overview – Scenarios

### Applicability
- Event-driven tasks
- Timed tasks
- Delay-insensitive tasks

### Inapplicability
- Start delay-sensitive tasks
- Processing delay-sensitive tasks
Serverless Platform Construction – Challenges

- Secure
- Multi-Tenancy
- Performance
- Cost
## Serverless Platform Construction – Solutions

### Problems

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>a</td>
<td>Operational Performance</td>
</tr>
<tr>
<td>b</td>
<td>Strong isolation of network access Interconnection</td>
</tr>
<tr>
<td>c</td>
<td>Strong isolation at runtime Millisecond level creation</td>
</tr>
</tbody>
</table>

### Solutions

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>a</td>
<td>Elastic Bare Metal Instance</td>
</tr>
<tr>
<td>b</td>
<td>VPC Network</td>
</tr>
<tr>
<td>c</td>
<td>Secure Containers</td>
</tr>
</tbody>
</table>
Serverless Platform Construction – Solutions

Relationships

- Tenant -> k8s namespace (1:n)
- k8s namespace -> VPC (1:1)
- VPC -> k8s namespace (1:n)
Kata Containers – Strong Isolation

Kata Shim V2

Kubernetes

OCI cmd/spec

IO

gRPC

gRPC

Virtual Machine

Container Command

Container Exec

Namespaces

Agent

Kernel

Hypervisor

Hypervisor VSOCK Socket
Kata Containers – Network Isolation

Shenlong ENI provides network isolation
Problem of 9pfs
1. Poor IO performance
2. Cause qemu hang

Two way to optimize IO
1. qcow2, good kernel compatibility
2. devicemapper, only stable on 4.19 kernel
Kata Container – Monitoring

Diagram:
- Kubelet
  - /stats/pod/container
  - Containerd
    - metric plugin
    - Containerd-shim-runc
      - cgroup from host
      - RunC container
    - Containerd-shim-kata
      - shim v2 interface Stats
      - Kata container
    - Containerd-shim-gvisor
      - gvisor container

Question mark indicating uncertainty.
Alibaba Cloud Serverless App Engine

Product Intro

EDAS Serverless用户群
446人
Coming Soon：ACK Secure Containers
Thanks