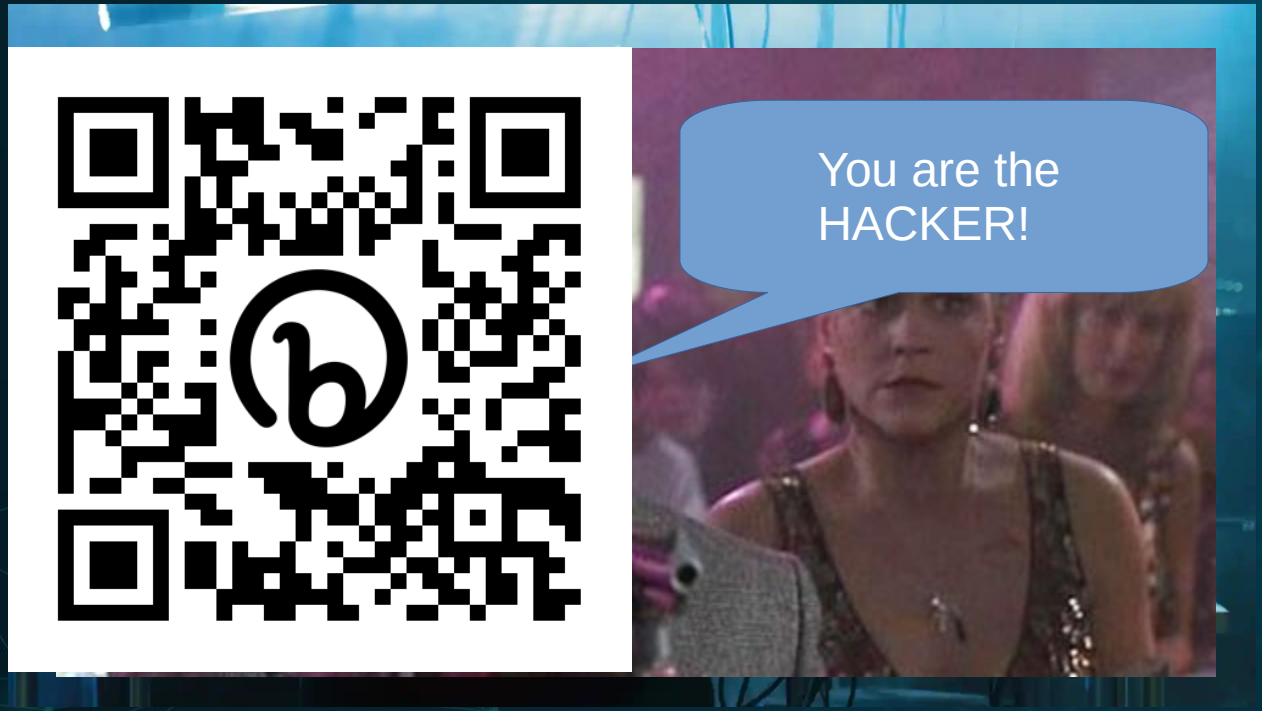
OpenInfra

The Hacker are hunting you

But why Containers and Infra-as-Code?


You are the HACKER!

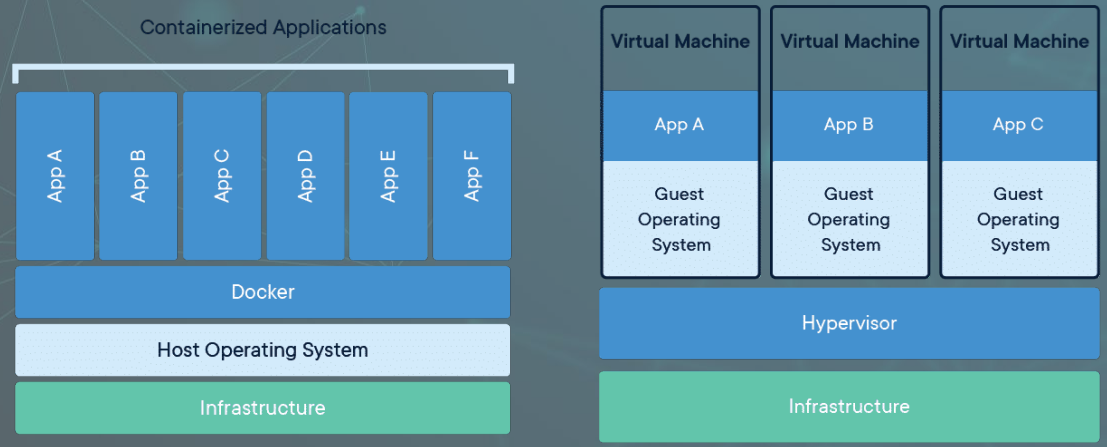
“Background”

01

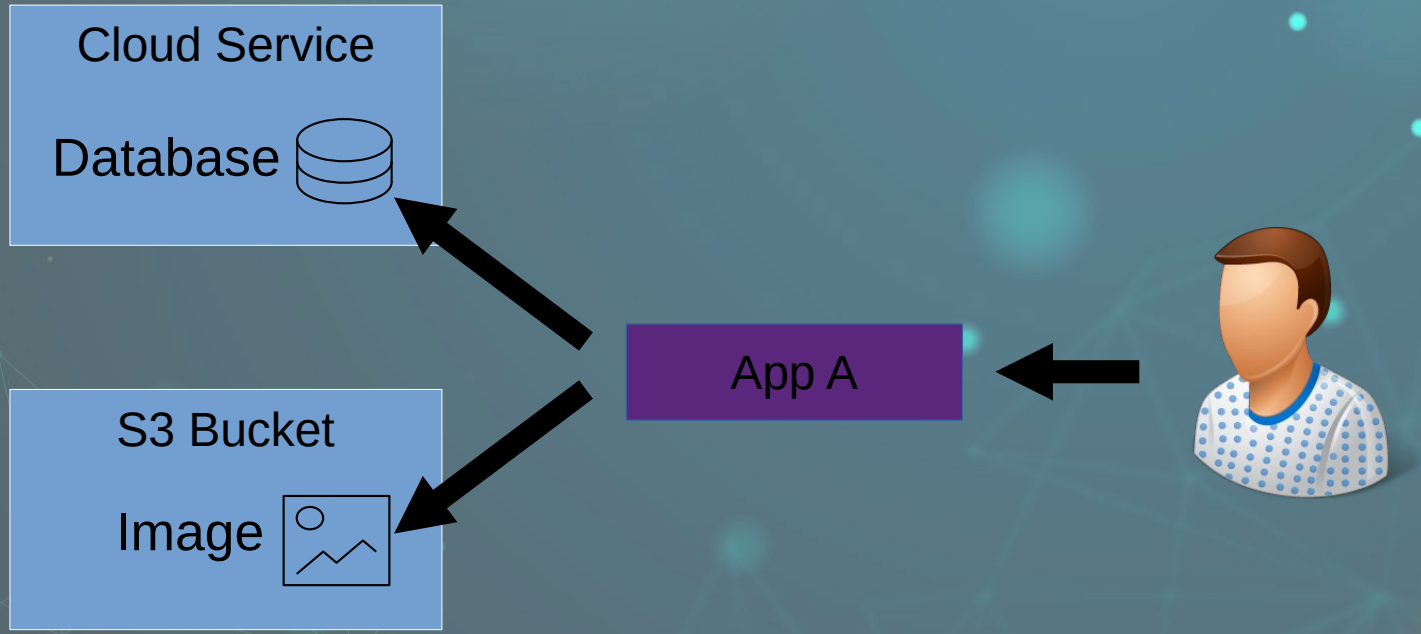
What is a Container

What is a container

A container is a standard unit of software that packages up code and all its dependencies so the application runs quickly and reliably from one computing environment to another. A Docker container image is a lightweight, standalone, executable package of software that includes everything needed to run an application: code, runtime, system tools, system libraries and settings. Container images become containers at runtime and in the case of Docker containers – images become containers when they run on Docker Engine. Available for both Linux and Windows-based applications, containerized software will always run the same, regardless of the infrastructure. Containers isolate software from its environment and ensure that it works uniformly despite differences for instance between development and staging.



How does it works



“Why Backup”

02

Everyone want to be the new kid in the block

What about the cool kid

How does it works now?

Persistence Volume

Database

App A

NFS Storage

Image

How do we backup that?

“Let’s Backup”

03

How can we backup the data?

Guidelines

- **3-2-1 Rule**
  - 3 Copies of your data
  - On 2 Different media
  - With 1 copy being off-line
- **Enable MFA**
- **Immutable filesystem**
- **Not a member of LDAP**

Who can help me

There is plenty of tools out there that can do “backup”, but what should you look for?

- Cohesity
- Rubrik
- OpenEBS
- Portworx
- Rancher Longhorn
- Velero
- IBM Spectrum Protect Plus
- Veeam Kasten
- Commvault

Alternative

Local and Global High-Availability

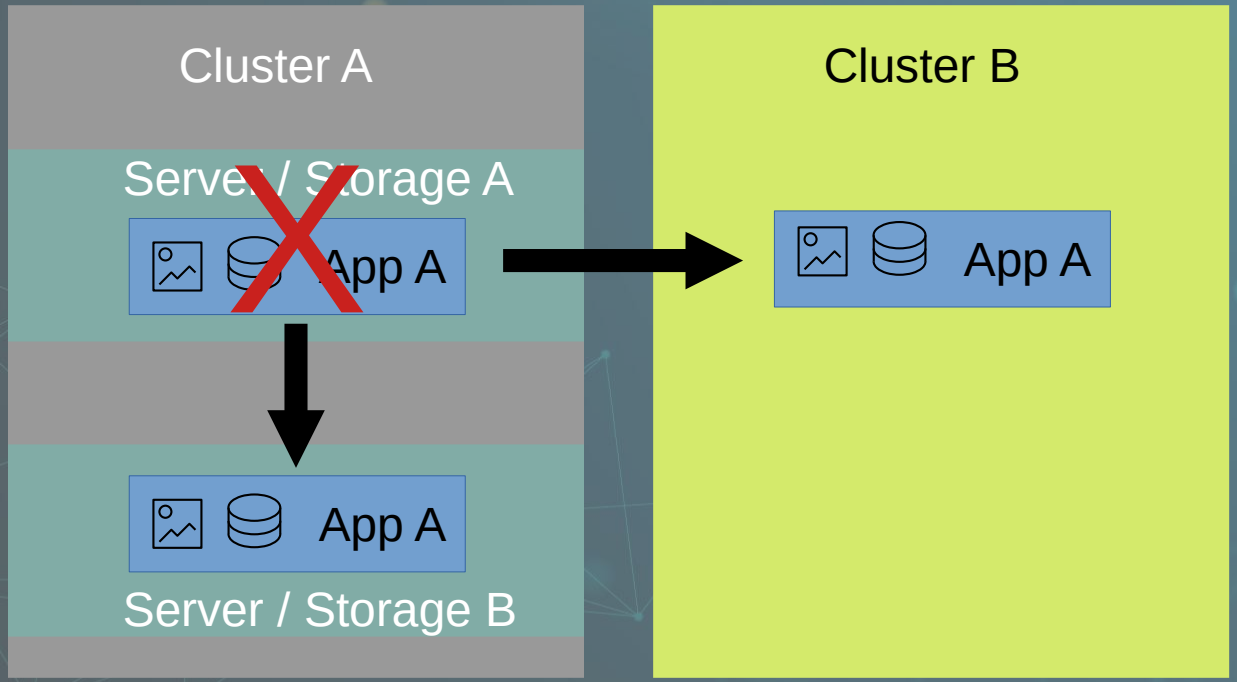
Local Snapshot

Backup and Restore

Disaster Recovery

Threat Recovery

Local / Global HA



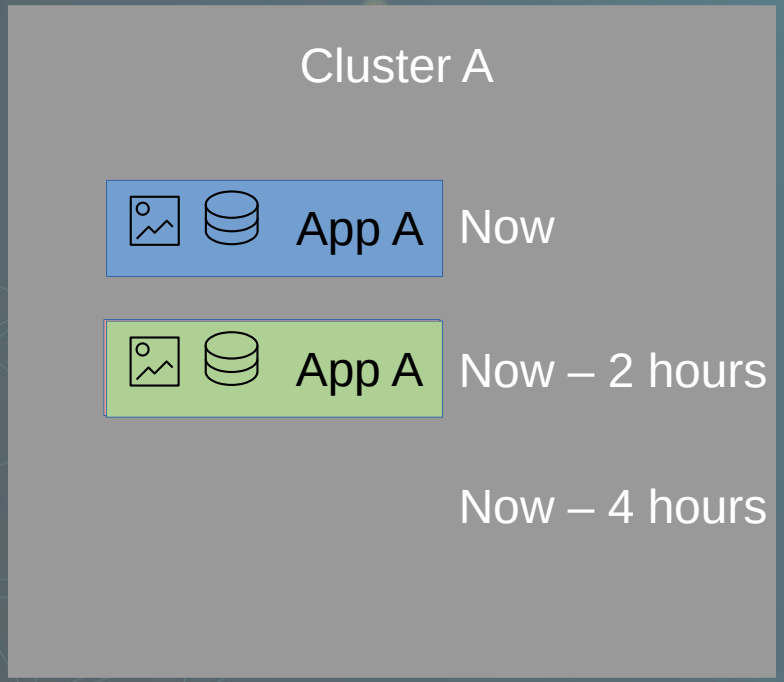
Pros

- Quick fail-over
- Low RTO

Cons

- No RPO
- No Compliance
- Replicate deleted data
- No Versioning of data
- Use a lot of Storage

Snapshot



Pros

- Low RTO
- High RPO

Cons

- Locally only
- No protection against Hardware failure
- No good protection against Ransomware

Backup and Recovery

Backup and Restore

- Get the data outside of the cluster
- Can restore data to the same cluster
- Can be bad RPO and RTO depending on backup application

Disaster Recovery

- Same as Backup and Restore
- Can restore data to another cluster including etcd meta-data

Threat Recovery

Threat Recovery
- Same as Disaster Recovery
- But you can also identify the threat inside the backup

Backup-as-Code
- Same as Threat Recovery, but you don’t need to spend days to identify
- Build everything as code, great complement with DevOps and Infra-as-code
- You can recover all containers everywhere

“Next Threat Level”

04

What is the next threat level

We hunt your code

THANKS!

Do you have any questions?

sales@isstech.io
Isstech.io